明 細 書

電子機器のためのセキュリティシステム

技術分野

[0001] 本発明は、例えばテレビジョン受像機とDVDレコーダとの間など、複数の電子機器のためのセキュリティシステムとその電子機器に関する。

背景技術

[0002] 従来の電子機器の盗難防止対策として、例えば、特許文献1において、以下の盗難防止装置が開示されている。例えば音響機器の盗難予防のために予めパスワードを設定してそれを不揮発性メモリに記憶させておき、次回の電源オン時にユーザーにパスワードの入力を求め、入力されたパスワードが不揮発性メモリに記憶させた内容と一致した場合に通常通り電源オンさせ、一致しなかった場合には、音響機器を動作させない。この装置では、そのパスワードの読み取り手法にも工夫を加えてセキュリティの強化を行っている。

[0003] 図2は、従来技術に係る特許文献1に記載された盗難防止装置を示すものである。図2において、当該盗難防止装置は、音響機器103の動作を制御するマイクロプロセッサ101と、所定のシステムの情報を保存する不揮発性メモリ102と、音響機器103とを備えて構成される。

[0004] ここで、マイクロプロセッサ101は、電源オン時のパスワードを予め設定する設定メニューを画面上でユーザーに提供し、その設定メニューでユーザーが入力したパスワードを不揮発性メモリ102に記憶して登録する。パスワードの登録後、ユーザーが音響機器103の電源をオンすると、マイクロプロセッサ101は、音響機器103を動作させる前にパスワード入力画面を表示し、ユーザーにパスワードの入力を求める。マイクロプロセッサ101は、入力されたパスワードが不揮発性メモリ102に記憶させたパスワードと一致すれば、音響機器103を通常通り動作させる。一方、パスワードが一致しなければ、盗難防止のために当該音響機器103の動作を中止する。なお、当該盗難防止装置では、不揮発性メモリ102に記憶されたパスワードを容易に読み取られない工夫が施されている。

[0005] 特許文献1:日本国特許出願公開平成2年042823号公報

発明の開示

発明が解決しようとする課題

[0006] しかしながら、上記従来技術に係る盗難防止装置では、ユーザーが音響機器103の電源を入れる毎に、毎回パスワードの入力が必要となり、ユーザーに煩雑な操作を強要することになる。また、パスワードを登録した本人しか音響機器103を動作させることができないという問題点があった。

[0007] 本発明の目的は以上の問題点を解決し、電子機器の電源をオンする毎にパスワードを入力する必要はなく、盗難防止などのセキュリティを強化できる電子機器のためのセキュリティシステムとその電子機器を提供することにある。

課題を解決するための手段

[0008] 第1の発明に係る電子機器のためのセキュリティシステムは、機器制御ラインを介して接続された、第1の電子機器と第2の電子機器を含む複数の電子機器のためのセキュリティシステムであって、

上記第2の電子機器は、パスワードを予め格納した第2の記憶手段を備え、

上記第1の電子機器は、

パスワードを予め格納した第1の記憶手段と、

上記第1の電子機器の起動時に、上記第2の電子機器に対して上記第2の記憶手段に格納されたパスワードを送信するように要求し、上記第2の電子機器からのパスワードを受信し、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、一致したとき、上記第1の電子機器の動作を開始させるようにセキュリティ機能を実行する制御手段とを備えたことを特徴とする。

[0009] 上記電子機器のためのセキュリティシステムにおいて、上記制御手段は、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき、上記第1の電子機器の動作を停止させるようにセキュリティ機能を実行することを特徴とする。

[0010] また、上記電子機器のためのセキュリティシステムにおいて、上記第1の電子機器は、ユーザーに対するメッセージを表示する表示手段と、パスワードを入力するため

の入力手段とをさらに備え、

上記制御手段は、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき、ユーザーに対してパスワードの入力を要求するように上記表示手段に表示し、上記ユーザーにより上記入力手段を用いて入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、一致したとき上記第1の電子機器の動作を開始させることを特徴とする。

[0011] さらに、上記電子機器のためのセキュリティシステムにおいて、上記制御手段は、上記ユーザーにより入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき上記第1の電子機器の動作を停止させることを特徴とする。

[0012] またさらに、上記電子機器のためのセキュリティシステムにおいて、上記制御手段は、上記ユーザーにより所定の複数回入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき上記第1の電子機器の動作を停止させることを特徴とする。

[0013] 上記電子機器のためのセキュリティシステムにおいて、上記第1の電子機器は、上記パスワードとは別の特別パスワードを予め格納した第3の記憶手段をさらに備え、

上記制御手段は、上記入力されたパスワードを、上記第3の記憶手段に格納された特別パスワードと比較して、一致したとき、上記第1の電子機器の動作を開始させることを特徴とする。

[0014] また、上記電子機器のためのセキュリティシステムにおいて、上記第1の電子機器は、

上記第1の電子機器に上記第2の電子機器が上記機器制御ラインを介して接続されているか否かを検出する第1の検出手段と、

上記第1の検出手段により上記第1の電子機器に上記第2の電子機器が接続されていることを検出したとき、上記機器制御ラインの制御信号を用いて、上記第2の電子機器がセキュリティ機能を有するか否かを検出する第2の検出手段とをさらに備え、

上記制御手段は、上記第1の電子機器の動作中において上記第1の検出手段と上

記第2の検出手段の処理を実行することを特徴とする。

[0015] さらに、上記電子機器のためのセキュリティシステムにおいて、例えばセキュリティ機能が設定されていないとき、上記制御手段は、上記第1の検出手段により上記第1の電子機器に上記第2の電子機器が接続されていないことを検出したとき、上記セキュリティ機能の処理を停止し、上記第1の電子機器の通常動作を開始させることを特徴とする。

[0016] またさらに、上記電子機器のためのセキュリティシステムにおいて、上記制御手段は、上記第2の検出手段により上記第2の電子機器が上記セキュリティ機能を有しないことを検出したとき、上記セキュリティ機能の処理を停止し、上記第1の電子機器の通常動作を開始させることを特徴とする。

[0017] 第2の発明に係るセキュリティシステムのための電子機器は、機器制御ラインを介して接続された、第1の電子機器と第2の電子機器を含む複数の電子機器のためのセキュリティシステムに設けられた第1の電子機器であって、

上記第2の電子機器は、パスワードを予め格納した第2の記憶手段を備え、

上記第1の電子機器は、

パスワードを予め格納した第1の記憶手段と、

上記第1の電子機器の起動時に、上記第2の電子機器に対して上記第2の記憶手段に格納されたパスワードを送信するように要求し、上記第2の電子機器からのパスワードを受信し、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、一致したとき、上記第1の電子機器の動作を開始させるようにセキュリティ機能を実行する制御手段とを備えたことを特徴とする。

[0018] 上記セキュリティシステムのための電子機器において、上記制御手段は、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき、上記第1の電子機器の動作を停止させるようにセキュリティ機能を実行することを特徴とする。

[0019] また、上記セキュリティシステムのための電子機器において、上記第1の電子機器は、ユーザーに対するメッセージを表示する表示手段と、パスワードを入力するための入力手段とをさらに備え、

上記制御手段は、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき、ユーザーに対してパスワードの入力を要求するように上記表示手段に表示し、上記ユーザーにより上記入力手段を用いて入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、一致したとき上記第1の電子機器の動作を開始させることを特徴とする。

[0020] さらに、上記セキュリティシステムのための電子機器において、上記制御手段は、上記ユーザーにより入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき上記第1の電子機器の動作を停止させることを特徴とする。

[0021] またさらに、上記セキュリティシステムのための電子機器において、上記制御手段は、上記ユーザーにより所定の複数回入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき上記第1の電子機器の動作を停止させることを特徴とする。

[0022] 上記セキュリティシステムのための電子機器において、上記第1の電子機器は、上記パスワードとは別の特別パスワードを予め格納した第3の記憶手段をさらに備え、

上記制御手段は、上記入力されたパスワードを、上記第3の記憶手段に格納された特別パスワードと比較して、一致したとき、上記第1の電子機器の動作を開始させることを特徴とする。

[0023] また、上記セキュリティシステムのための電子機器において、上記第1の電子機器は、

上記第1の電子機器に上記第2の電子機器が上記機器制御ラインを介して接続されているか否かを検出する第1の検出手段と、

上記第1の検出手段により上記第1の電子機器に上記第2の電子機器が接続されていることを検出したとき、上記機器制御ラインの制御信号を用いて、上記第2の電子機器がセキュリティ機能を有するか否かを検出する第2の検出手段とをさらに備え、

上記制御手段は、上記第1の電子機器の動作中において上記第1の検出手段と上記第2の検出手段の処理を実行することを特徴とする。

[0024] さらに、上記セキュリティシステムのための電子機器において、上記制御手段は、上記第1の検出手段により上記第1の電子機器に上記第2の電子機器が接続されていないことを検出したとき、上記セキュリティ機能の処理を停止し、上記第1の電子機器の通常動作を開始させることを特徴とする。

[0025] またさらに、上記セキュリティシステムのための電子機器において、例えばセキュリティ機能が設定されていないとき、上記制御手段は、上記第2の検出手段により上記第2の電子機器が上記セキュリティ機能を有しないことを検出したとき、上記セキュリティ機能の処理を停止し、上記第1の電子機器の通常動作を開始させることを特徴とする。

発明の効果

[0026] 従って、本発明に係る電子機器のためのセキュリティシステムによれば、機器制御ラインを介して接続された複数の電子機器のためのセキュリティシステムにおいて、接続された補助装置の電子機器の記憶手段にパスワードを登録することによって、主装置の電子機器の起動時にそのパスワードを確認することができるので、機器制御ラインが接続されている限りにおいて、主装置の電子機器と補助装置の電子機器との間でパスワードが一致すれば、ユーザーにとって通常の電源オン時の処理と同様に、当該電子機器が起動開始できる。補助装置の電子機器が接続されていないときは、主装置の電子機器を起動できないので、主装置の電子機器が盗難されても起動することができない。それ故、ユーザーにパスワードの入力など煩雑な操作を強いることなく盗難防止を実現できる。さらに、このシステムはほとんどコストアップなしに実現できるという特有の効果を有する。

図面の簡単な説明

[0027] [図1]本発明の実施形態に係る、テレビジョン受像機201とDVDレコーダ205を含むセキュリティシステムの構成を示すブロック図である。

[図2]従来技術に係る盗難防止装置の構成を示すブロック図である。

[図3]図1のコントローラ202とコントローラ206との間の通信手順P1を示すシーケンス図である。

[図4]図1のコントローラ202とコントローラ206との間の通信手順P2を示すシーケン

ス図である。

[図5]図1のコントローラ202とコントローラ206との間の通信手順P3を示すシーケンス図である。

[図6]図1のコントローラ202とコントローラ206との間の通信手順P4を示すシーケンス図である。

[図7]図1のコントローラ202によって実行される出荷後最初の電源オン時処理を示すフローチャートである。

[図8]図7のサブルーチンであるセキュリティ機能確認処理(ステップS9)を示すフローチャートである。

[図9]図1のコントローラ202によって実行される機器制御処理の第1の部分を示すフローチャートである。

[図10]図1のコントローラ202によって実行される機器制御処理の第2の部分を示すフローチャートである。

[図11]図1のコントローラ202によって実行される機器制御処理の第3の部分を示すフローチャートである。

[図12]図9のサブルーチンであるオーナーIDの再登録時処理(ステップS28)の第1の部分を示すフローチャートである。

[図13]図9のサブルーチンであるオーナーIDの再登録時処理(ステップS28)の第2の部分を示すフローチャートである。

[図14]図9のサブルーチンであるオーナーIDの再登録時処理(ステップS28)の第3の部分を示すフローチャートである。

[図15]図10の処理の変形例を示すフローチャートである。

[図16]図11の処理の変形例を示すフローチャートである。

[図17]図12の処理の変形例を示すフローチャートである。

[図18]図7のステップS1の処理で表示されるスタート時自動セットアップの画面D1を示す正面図である。

[図19]図7のステップS2の処理で表示される初期電源オン時登録の画面D2を示す正面図である。

[図20]図7のステップS8の処理で表示されるセキュリティオプションの使用の確認(その1)の画面D3を示す正面図である。

[図21]図7のステップS14の処理で表示されるセキュリティオプションの使用の確認(その2)の画面D4を示す正面図である。

[図22]図7のステップS15の処理で表示されるセキュリティオプションの使用の確認(その3)の画面D5を示す正面図である。

[図23]図7のステップS19の処理で表示されるセキュリティオプションの使用の確認(その4)の画面D6を示す正面図である。

[図24]図7のステップS12の処理で表示されるセキュリティオプションの使用の確認(その5)の画面D7を示す正面図である。

[図25]図11のステップS41の処理で表示されるセキュリティ機能は機器接続の消失により動作中であることの通知(その1)の画面D8を示す正面図である。

[図26]図11のステップS45の処理で表示されるセキュリティ機能は機器接続の消失により動作中であることの通知(その2)の画面D9を示す正面図である。

[図27]図10のステップS31の処理で表示されるセキュリティ機能は機器接続の変更により動作中であることの通知(その1)の画面D10を示す正面図である。

[図28]図10のステップS35の処理で表示されるセキュリティ機能は機器接続の変更により動作中であることの通知(その2)の画面D11を示す正面図である。

[図29]図12のステップS51の処理で表示されるPIN番号が登録された後のオーナーIDメニューの画面D12を示す正面図である。

[図30]図12のステップS56の処理で表示される間違ったPIN番号が入力されたときのオーナーIDメニューの画面D13を示す正面図である。

[図31]図13のステップS65乃至S68の処理で表示される名前、家屋番号、ポストコード又はセキュリティ機能の変更後のオーナーIDメニューの画面D14を示す正面図である。

[図32]図13のステップS65乃至S68の処理で表示される名前、家屋番号、ポストコード又はセキュリティ機能の変更後のオーナーIDメニューの画面D15を示す正面図である。

[図33]図13のステップS69乃至S70の処理で表示される名前、家屋番号又はポストコードの変更後のオーナーIDメニューの画面D16を示す正面図である。

[図34]図7のステップS10の処理で表示される通常選局画面である画面D17を示す正面図である。

符号の説明

[0028] 201…テレビジョン受像機、

202…コントローラ、

203…不揮発性メモリ、

203A…ROM、

204…映像信号及び音声信号処理回路、

204A…ディスプレイ、

205…DVDレコーダ、

206…コントローラ、

207…不揮発性メモリ、

208…映像信号及び音声信号処理回路、

208A…DVDドライブ装置、

209…機器制御ライン、

210…映像信号ライン、

211…音声信号ライン、

220…赤外線信号受信機、

221…リモートコントローラ、

222…キーボード、

223…赤外線信号送信機。

発明を実施するための最良の形態

[0029] 以下、本発明に係る実施形態について図面を参照して説明する。

[0030] 図1は、本発明の実施形態に係る、テレビジョン受像機201とDVDレコーダ205を含むセキュリティシステムの構成を示すブロック図である。本実施形態に係るセキュリティシステムは、機器制御ライン209を介して接続された、テレビジョン受像機201と

、DVDレコーダ205とを備えて構成される。ここで、DVDレコーダ205はパスワードを予め格納した不揮発性メモリ207を含む。テレビジョン受像機201はパスワードを予め格納した不揮発性メモリ203とコントローラ202とを含む。コントローラ202はテレビジョン受像機201の起動時に、図6の通信手順P4を用いて、DVDレコーダ205に対して不揮発性メモリ207に格納されたパスワードを送信するように要求し、DVDレコーダ205からのパスワードを受信し、受信されたパスワードを、不揮発性メモリ203内のパスワードと比較して(図9のステップS25)、一致したとき(ステップS26でYES)テレビジョン受像機201の動作を開始させる(ステップS26A)ことを特徴としている。本実施形態では、パスワードとして、PIN番号(Personal Identification Number)を用いる。

[0031] 図1において、主装置であるテレビジョン受像機201は、その動作を制御するコントローラ202と、パスワードであるPIN番号などのデータを格納する、例えばEEPROM又はフラッシュメモリなどの不揮発性メモリ203と、例えばカスタマーエンジニア用特別PIN番号などのデータを格納するROM(読み出し専用メモリ)203Aと、映像信号及び音声信号処理回路204と、ディスプレイ204Aと、リモートコントローラ221の赤外線信号送信機223からの赤外線信号を受信する赤外線信号受信機220とを備えて構成される。また、テレビジョン受像機201には、その動作をユーザーが遠隔制御するためのリモートコントローラ221が付属されており、リモートコントローラ221は、パスワードや選局データなどのデータを入力するためのキーボード222と、入力されたデータを赤外線信号受信機220に送信する赤外線信号送信機223とを備えて構成される。

[0032] DVDレコーダ205は、その動作を制御するコントローラ206と、コントローラ206に接続されパスワードであるPIN番号やセキュリティ機能を有するか否かの情報などのデータを格納する、例えばEEPROM又はフラッシュメモリなどの不揮発性メモリ203と、映像信号及び音声信号処理回路208と、DVDドライブ装置208Aとを備えて構成される。ここで、テレビジョン受像機201のコントローラ202と、DVDレコーダ205のコントローラ206との間は、例えば、欧州における電子機器において用いられる21ピンスカートケーブル、HDMI(High Definition Multimedia Interface)ケーブル、IEEE

1394に準拠した制御ケーブルなど電子機器間の制御に用いるための機器制御ライン209を介して接続されており、コントローラ202，206はその間で図3乃至図6を参照して説明する通信手順P1乃至P4を用いて種々の信号を送受信する。本実施形態において、当該機器制御ライン209を用いた接続を、「機器接続」という。また、映像信号及び音声信号処理回路204と、映像信号及び音声信号処理回路208との間は、映像信号ライン210及び音声信号ライン211とにより接続されている。映像信号及び音声信号処理回路208は、コントローラ206によりその動作が制御され、DVDドライブ装置208Aで再生された映像信号及び音声信号に対して所定の信号処理を実行した後、映像信号ライン210及び音声信号ライン211を介して映像信号及び音声信号処理回路204に送信する。

[0033] テレビジョン受像機201に付属されたリモートコントローラ221において、キーボード222は、例えば図19の画面D2に示すように、中央キーを含む十字キー、テンキー、機能キーなどを含む。ユーザーはキーボード222を用いてパスワードや選局情報などのデータを入力し、当該データは赤外線信号送信機223により赤外線信号受信機220に無線送信された後、コントローラ202に出力される。不揮発性メモリ203に格納されたPIN番号などのデータはコントローラ202により読み出され、ROM203Aに格納された特別PIN番号などのデータはコントローラ202により読み出される。映像信号及び音声信号処理回路204は、コントローラ202によりその動作が制御され、映像信号及び音声信号処理回路208からの映像信号及び音声信号を受信して、それらに対して所定の信号処理を実行した後、ディスプレイ204A及びスピーカ（図示せず。）に出力する。

[0034] 次いで、図3乃至図6を参照して、主装置であるテレビジョン受像機201のコントローラ202と、補助装置であるDVDレコーダ205のコントローラ206との間で機器制御ライン209を介して実行される種々の通信手順P1乃至P4について以下に説明する。

[0035] 図3は図1のコントローラ202とコントローラ206との間の通信手順P1を示すシーケンス図である。図3において、コントローラ202は、接続確認信号をコントローラ206に送信し、これに応答して、コントローラ206は、当該接続確認信号を受信したときに接

続確認ACK信号（ACKは肯定応答（Acknowledgment）の略である。）をコントローラ202に返信する。これにより、機器制御ライン209を介した機器接続が正常に接続されていることを確認できる。

[0036] 図4は図1のコントローラ202とコントローラ206との間の通信手順P2を示すシーケンス図である。図4において、コントローラ202は、セキュリティ機能確認信号をコントローラ206に送信し、これに応答して、コントローラ206は、DVDレコーダ205がセキュリティ機能を有しているか否かの情報を不揮発性メモリ207から読み出して、セキュリティ機能を有しているときにセキュリティ機能ACK信号をコントローラ202に返信する一方、セキュリティ機能を有していないときにセキュリティ機能ACK信号をコントローラ202に返信しない。これにより、DVDレコーダ205がセキュリティ機能を有しているか否かを確認できる。

[0037] 図5は図1のコントローラ202とコントローラ206との間の通信手順P3を示すシーケンス図である。図5において、コントローラ202は、書き込むべきパスワードを含むパスワード書込要求信号をコントローラ206に送信し、これに応答して、コントローラ206は、パスワード書込要求信号に含まれるパスワードを不揮発性メモリ207に書き込んだ後、パスワード書込ACK信号をコントローラ202に返信する。これにより、コントローラ202からコントローラ206を介して不揮発性メモリ207にパスワードを書き込むことができ、その結果を確認できる。

[0038] 図6は図1のコントローラ202とコントローラ206との間の通信手順P4を示すシーケンス図である。図6において、コントローラ202は、不揮発性メモリ207に格納されたパスワードを要求するパスワード書込要求信号をコントローラ206に送信し、これに応答して、コントローラ206は、不揮発性メモリ207に格納されたパスワードを読み出し、当該パスワードを含むパスワード返信信号をコントローラ202に返信する。これにより、コントローラ202からコントローラ206を介して不揮発性メモリ207に格納されたパスワードを読み出して受信できる。

[0039] 図7は図1のコントローラ202によって実行される出荷後最初の電源オン時処理を示すフローチャートである。なお、以下のすべての制御処理において、画面はすべてディスプレイ204Aに表示される。また、図18乃至図34にそれぞれ図示された画面

D1乃至D17はそれぞれ一例を示している。

[0040] 図7において、まず、ステップS1で、図18の画面D1を表示して、自動チューニングプリセット処理を含む自動セットアップ処理を実行し、ステップS2においてユーザー登録画面であるオーナーID(Identification)画面である図19の画面D2を表示する。次いで、ユーザーは、画面D2上でPIN番号(4桁数字)、名前、住所、郵便番号を含むユーザー登録情報をキーボード222を用いて入力する。そして、ステップS4において通信手順P1により機器接続を確認し、ステップS5において機器接続はOKか否かが判断され、YESのときはステップS6に進む一方、NOのときはステップS10に進む。ステップS6において通信手順P2により接続機器であるDVDレコーダ205のセキュリティ機能を確認し、ステップS7において接続機器はセキュリティ接続機器を有するか否かが判断され、YESのときはステップS8に進む一方、NOのときはステップS10に進む。ステップS8において、セキュリティ機能の使用確認画面(図20の画面D3)を表示し、ステップS9のセキュリティ機能確認処理(図8)において、ユーザーに対してセキュリティ機能を使用するか否かの確認を行い、ステップS10に進む。ユーザーがセキュリティ機能を使用するときは、画面D3においてYESを選択し、使用しないときは画面D3においてNOを選択する。ステップS10において、図34の画面D17に示すように、通常選局画面で番組ポジション"1"を選局した後、当該処理を終了して通常処理(例えば、図9のステップS29に進む。)を実行する。

[0041] 図7において、機器接続が未接続で(ステップS5でNO)、又は接続機器がセキュリティ機能を有しないとき(ステップS7でNO)、セキュリティ機能確認処理に入らないので、セキュリティ機能に関する入力項目を表示することを停止し、ユーザーに対して、当該テレビジョン受像機201がセキュリティ機能が存在することを告知しない。これにより、ユーザーに対して余分な情報を与えず、その操作も簡単化できる。

[0042] 図8は図7のサブルーチンであるセキュリティ機能確認処理(ステップS9)を示すフローチャートである。

[0043] 図8において、まず、ステップS11においてセキュリティ機能を使用するか否かが判断され、ステップS12において、図24の画面D7に示すように、セキュリティ機能を使用しないことを示すメッセージを2秒間表示し、セキュリティフラグSFを0にリセットした

後、元のメインルーチンに戻る。ここで、セキュリティフラグSFは、0に設定されたときセキュリティ機能を使用することを示す一方、1に設定されたときセキュリティ機能を使用しないことを示す。一方、ステップS14において、セキュリティ機能を使用するという選択の再確認の画面D4(図21)を表示し、OKであるときに、ステップS15において使用するという選択の再々確認の画面D5(図22)を表示し、さらにOKであるときに、ステップS16に進む。ステップS16において、通信手順P3により、ステップS3で入力されたPIN番号を不揮発性メモリ207に書き込むようにコントローラ206に指示し、ステップS17においてパスワードACK信号を受信したか否かが判断され、YESとなるまでステップS17の処理を繰り返し、YESとなったときに、ステップS18において、不揮発性メモリ203にPIN番号を書き込む。そして、ステップS19において、図23の画面D6に示すように、セキュリティ機能が組み込まれたことを示すメッセージを2秒間表示し、セキュリティフラグSFを1にセットした後、元のメインルーチンに戻る。

[0044] 図9乃至図11は、図1のコントローラ202によって実行される機器制御処理を示すフローチャートである。

[0045] 図9のステップS21において通信手順P1により機器接続を確認し、ステップS22において機器接続はOKか否かが判断され、YESのときはステップS23に進む一方、NOのときは図11のステップS41に進む。ステップS23において通信手順P2により接続機器であるDVDレコーダ205のセキュリティ機能の有無を確認し、ステップS24においてセキュリティ機能を有するか否かが判断され、YESのときはステップS25に進む一方、NOのときは図10のステップS31に進む。ステップS25において、通信手順P4により不揮発性メモリ207内のPIN番号の送信を要求してコントローラ206から機器制御ライン209を介して当該PIN番号を受信し、受信したPIN番号を、不揮発性メモリ203内のPIN番号を比較する。ステップS26においてこれらのPIN番号は一致するか否かが判断され、YESのときはステップS26Aに進む一方、NOのときは図10のステップS31に進む。ステップS26Aにおいて、映像信号及び音声信号処理回路204の動作を開始し、又は動作可能状態を継続させ、ステップS27において、所定のメニュー画面においてオーナーIDメニューを選択したか否かが判断され、YESのときはステップS28に進む一方、NOのときはステップS29に進む。ステップS28で

は、図12乃至図14のオーナーID再登録処理を実行した後、ステップS21に戻る。ステップS29においてその他の通常処理を実行した後、ステップS21に戻る。

[0046] 図10のステップS31においては、図27の画面D10に示すように、接続機器が変更されたことを示すメッセージを表示し、セキュリティ機能をキャンセルするためのPIN番号の入力(4桁数字)を促し、ステップS32においてPIN番号を入力したか否かが判断され、YESのときはステップS33に進む一方、NOのときはステップS32に戻る。ステップS33において入力されたPIN番号と不揮発性メモリ203内のPIN番号を比較し、ステップS34においてこれらのPIN番号は一致するか否かが判断され、YESのときはステップS36に進む一方、NOのときはステップS35に進む。ステップS35において映像信号及び音声信号処理回路204の動作を停止し、図28の画面D11に示すように、PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求し、ステップS32に戻る。さらに、ステップS36では、映像信号及び音声信号処理回路204の動作を開始し、ステップS37においてセキュリティフラグSFを0にリセットすることによりセキュリティ機能をキャンセルした後、図9のステップS29に進む。

[0047] さらに、図11のステップS41において、図25の画面D8に示すように、接続機器が切り離されたために、セキュリティ機能が動作していることを知らせるメッセージを表示し、セキュリティ機能をキャンセルしたい場合は、PIN番号を入力するように促し、ステップS42においてPIN番号を入力したか否かが判断され、YESのときはステップS43に進む一方、NOのときはステップS42に戻る。ステップS43において入力されたPIN番号と不揮発性メモリ203内のPIN番号を比較し、ステップS44においてこれらのPIN番号は一致するか否かが判断され、YESのときはステップS46に進む一方、NOのときはステップS45に進む。ステップS45において映像信号及び音声信号処理回路204の動作を停止し、図26の画面D9に示すように、PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求した後、ステップS42に戻る。ステップS46では、映像信号及び音声信号処理回路204の動作を開始し、ステップS47においてセキュリティフラグSFを0にリセットすることによりセキュリティ機能をキャンセルした後、図9のステップS29に進む。

[0048] 図12乃至図14は、図9のサブルーチンであるオーナーIDの再登録時処理(ステッ

プS28)を示すフローチャートである。

[0049] 図12のステップS51において、図29の画面D12に示すように、オーナーIDメニューを表示し、ステップS52においてPIN番号(4桁数字)を入力するように促し、ステップS53においてPIN番号を入力したか否かが判断され、YESのときはステップS54に進む一方、NOのときはステップS53に戻る。ステップS54において入力されたPIN番号と不揮発性メモリ203内のPIN番号を比較し、ステップS55においてこれらのPIN番号は一致するか否かが判断され、YESのときはステップS57に進む一方、NOのときはステップS56Aに進む。ステップS56Aでは、セキュリティフラグSFが1であるか否かが判断され、すなわち、セキュリティ機能が設定されているか否かが判断され、YESのときはステップS56Bに進む一方、NOのときはステップS56Cに進む。ステップS56Bでは、映像信号及び音声信号処理回路204の動作を停止し、次いで、ステップS56Cでは、図30の画面D13に示すように、PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求した後、ステップS53に戻る。ステップS57では、映像信号及び音声信号処理回路204の動作を開始し、図13のステップS61に進む。

[0050] 図13のステップS61において通信手順P1により機器接続を確認し、ステップS62において機器接続はOKか否かが判断され、YESのときはステップS63に進む一方、NOのときはステップS69に進む。ステップS63において通信手順P2によりDVDレコーダ205のセキュリティ機能の有無を確認し、ステップS64においてセキュリティ機能を有するか否かが判断され、YESのときはステップS65に進む一方、NOのときはステップS69に進む。ステップS65において、図31の画面D14に示すように、オーナーIDメニューに“セキュリティ機能”の項目を追加して表示し、ステップS66においてオーナーIDメニューで、PIN番号、名前、住所、郵便番号を再登録し、ステップS67で現在のセキュリティフラグSFの値を待避セキュリティフラグSF1に待避させる。さらに、ステップS68において画面D14又はD15上でセキュリティ機能のオン／オフの選択を行う。画面D14ではセキュリティ機能をオフに設定した場合を示し、画面D15ではセキュリティ機能をオンに設定した場合を示す。ここで、セキュリティ機能をオンしたときは、セキュリティフラグSFには1がセットされ、セキュリティ機能をオフしたときは

セキュリティフラグSFは0にリセットされる。そして、図14のステップS72に進む。

[0051] 図13のステップS69では、図33の画面D16に示すように、オーナーIDメニューに“セキュリティ機能”の項目を表示せず、ステップS70においてオーナーIDメニューで、PIN番号、名前、住所、郵便番号を再登録する。そして、ステップS71でセキュリティフラグSFを0にリセットし、図9のステップS29のその他の通常処理に進む。

[0052] 図13において、機器接続が未接続で(ステップS62でNO)、又は接続機器がセキュリティ機能を有しないとき(ステップS64でNO)、セキュリティ機能確認処理に入らないので、セキュリティ機能に関する入力項目を表示することを停止し、ユーザーに対して、当該テレビジョン受像機201がセキュリティ機能が存在することを告知しない。これにより、ユーザーに対して余分な情報を与えず、その操作も簡単化できる。

[0053] 図14のステップS72において、SF1＝0かつSF＝1であるか否かが判断され、すなわち、セキュリティ機能の設定がオフからオンに遷移したか否かが判断され、YESのときは図8のステップS14に進む一方、NOのときはステップS73に進む。ステップS73においてSF1＝1かつSF＝0であるか否かが判断され、すなわち、セキュリティ機能の設定がオンからオフに遷移したか否かが判断され、YESのときは図8のステップS12に進む一方、NOのときは図9のステップS29のその他の通常処理に進む。

[0054] 図15は図10の処理の変形例を示すフローチャートであり、図16は図11の処理の変形例を示すフローチャートであり、図17は図12の処理の変形例を示すフローチャートである。図15乃至図17の変形例では、ROM203A内に予め格納されたカスタマーエンジニア用特別PIN番号の一致処理と、所定の複数N回(例えば、Nは3回)以上雄PIN番号を入力して不一致であるときに、映像信号及び音声信号処理回路204の動作を停止する処理を追加したことを特徴としている。ここで、特別PIN番号は、ROM203Aに予め格納され、セキュリティ機能をキャンセルするためのパスワードとして、ユーザーが入力するPIN番号のほかに、製造者又は製造者から委託を受けて認証された例えばカスタマーエンジニアが特別PIN番号を入力することにより、セキュリティ機能を強制的にキャンセルして、当該テレビジョン受像機201の動作を開始させるために設けられる。

[0055] 図15の変形例において、ステップS34とステップS32との間にステップS38からス

テップS35Bまでの処理を挿入したことを特徴としている。ステップS34においてNOであるとき、ステップS38において、入力されたPIN番号とROM203A内の特別PIN番号を比較し、ステップS39でこれらのPIN番号が一致するか否かが判断され、YESのときはステップS36に進む一方、NOのときはステップS40に進む。ステップS40では、所定の複数N回以上PIN番号を入力しても不一致であるか否かが判断され、YESのときはステップS35Aに進む一方、NOのときはステップS35Bに進む。ステップS35Aでは、映像信号及び音声信号処理回路204の動作を停止し、ステップS35Bにおいて、図28の画面D11に示すように、PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求し、ステップS32に進む。

[0056] 図16の変形例において、ステップS44とステップS42との間にステップS48からステップS45Bまでの処理を挿入したことを特徴としている。ステップS44においてNOであるとき、ステップS48において、入力されたPIN番号とROM203A内の特別PIN番号を比較し、ステップS49でこれらのPIN番号が一致するか否かが判断され、YESのときはステップS46に進む一方、NOのときはステップS50に進む。ステップS50では、所定の複数N回以上PIN番号を入力しても不一致であるか否かが判断され、YESのときはステップS45Aに進む一方、NOのときはステップS45Bに進む。ステップS45Aでは、映像信号及び音声信号処理回路204の動作を停止し、ステップS45Bにおいて、図26の画面D9に示すように、PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求し、ステップS42に進む。

[0057] 図17の変形例において、ステップS55とステップS53との間にステップS58からステップS56Cまでの処理を挿入したことを特徴としている。ステップS55においてNOであるとき、ステップS58において、入力されたPIN番号とROM203A内の特別PIN番号を比較し、ステップS59でこれらのPIN番号が一致するか否かが判断され、YESのときはステップS57に進む一方、NOのときはステップS56Aに進む。ステップS56Aでは、セキュリティフラグSFが1であるか否かが判断され、すなわち、セキュリティ機能が設定されているか否かが判断され、YESのときはステップS60に進む一方、NOのときはステップS56Cに進む。ステップS60では、所定の複数N回以上PIN番号を入力しても不一致であるか否かが判断され、YESのときはステップS56Bに進む一

方、NOのときはステップS56Cに進む。ステップS56Bでは、映像信号及び音声信号処理回路204の動作を停止し、次いで、ステップS56Cにおいて、図28の画面D11に示すように、PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求し、ステップS53に進む。

[0058] 以上の実施形態においては、テレビジョン受像機201と、DVDレコーダ205とを含むセキュリティシステムについて開示しているが、本発明はこれに限らず、セキュリティシステムにおいて用いる電子機器は、これらに限定されず、テレビジョン受信機、セットトップボックス、ディスプレイ装置、DVDプレイヤなどの種々の電子機器を用いてもよい。また、3個以上の電子機器を機器制御ライン209を用いて接続してセキュリティシステムを構成してもよい。

[0059] 以上の実施形態では、赤外線信号を用いてユーザーによりキーボード222を用いて入力されたデータをコントローラ202に無線送信しているが、本発明はこれに限らず、キーボード222をテレビジョン受像機201の本体に設けてもよい。

[0060] 以上の実施形態においては、図9のステップS26においてNOであるときは、図10のステップS31に進むが、本発明はこれに限らず、その前に、ステップS35の一部の処理である「映像信号及び音声信号処理回路204の動作を停止する処理」を実行してもよい。

産業上の利用可能性

[0061] 以上詳述したように、本発明に係る電子機器のためのセキュリティシステムによれば、機器制御ラインを介して接続された複数の電子機器のためのセキュリティシステムにおいて、接続された補助装置の電子機器の記憶手段にパスワードを登録することによって、主装置の電子機器の起動時にそのパスワードを確認することができるので、機器制御ラインが接続されている限りにおいて、主装置の電子機器と補助装置の電子機器との間でパスワードが一致すれば、ユーザーにとって通常の電源オン時の処理と同様に、当該電子機器が起動開始できる。補助装置の電子機器が接続されていないときは、主装置の電子機器を起動できないので、主装置の電子機器が盗難されても起動することができない。それ故、ユーザーにパスワードの入力など煩雑な操作を強いることなく盗難防止を実現できる。さらに、このシステムはほとんどコストア

ップなしに実現できるという特有の効果を有する。

請求の範囲

[1] 機器制御ラインを介して接続された、第1の電子機器と第2の電子機器を含む複数の電子機器のためのセキュリティシステムであって、

上記第2の電子機器は、パスワードを予め格納した第2の記憶手段を備え、

上記第1の電子機器は、

パスワードを予め格納した第1の記憶手段と、

上記第1の電子機器の起動時に、上記第2の電子機器に対して上記第2の記憶手段に格納されたパスワードを送信するように要求し、上記第2の電子機器からのパスワードを受信し、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、一致したとき、上記第1の電子機器の動作を開始させるようにセキュリティ機能を実行する制御手段とを備えたことを特徴とする電子機器のためのセキュリティシステム。

[2] 上記制御手段は、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき、上記第1の電子機器の動作を停止させるようにセキュリティ機能を実行することを特徴とする請求項1記載の電子機器のためのセキュリティシステム。

[3] 上記第1の電子機器は、ユーザーに対するメッセージを表示する表示手段と、パスワードを入力するための入力手段とをさらに備え、

上記制御手段は、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき、ユーザーに対してパスワードの入力を要求するように上記表示手段に表示し、上記ユーザーにより上記入力手段を用いて入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、一致したとき上記第1の電子機器の動作を開始させることを特徴とする請求項1記載の電子機器のためのセキュリティシステム。

[4] 上記制御手段は、上記ユーザーにより入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき上記第1の電子機器の動作を停止させることを特徴とする請求項3記載の電子機器のためのセキュリティシステム。

[5] 上記制御手段は、上記ユーザーにより所定の複数回入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき上記第1の電子機器の動作を停止させることを特徴とする請求項3記載の電子機器のためのセキュリティシステム。

[6] 上記第1の電子機器は、上記パスワードとは別の特別パスワードを予め格納した第3の記憶手段をさらに備え、

上記制御手段は、上記入力されたパスワードを、上記第3の記憶手段に格納された特別パスワードと比較して、一致したとき、上記第1の電子機器の動作を開始させることを特徴とする請求項3乃至5のうちのいずれか1つに記載の電子機器のためのセキュリティシステム。

[7] 上記第1の電子機器は、

上記第1の電子機器に上記第2の電子機器が上記機器制御ラインを介して接続されているか否かを検出する第1の検出手段と、

上記第1の検出手段により上記第1の電子機器に上記第2の電子機器が接続されていることを検出したとき、上記機器制御ラインの制御信号を用いて、上記第2の電子機器がセキュリティ機能を有するか否かを検出する第2の検出手段とをさらに備え、

上記制御手段は、上記第1の電子機器の動作中において上記第1の検出手段と上記第2の検出手段の処理を実行することを特徴とする請求項1乃至6のうちのいずれか1つに記載の電子機器のためのセキュリティシステム。

[8] 上記制御手段は、上記第1の検出手段により上記第1の電子機器に上記第2の電子機器が接続されていないことを検出したとき、上記セキュリティ機能の処理を停止し、上記第1の電子機器の通常動作を開始させることを特徴とする請求項7記載の電子機器のためのセキュリティシステム。

[9] 上記制御手段は、上記第2の検出手段により上記第2の電子機器が上記セキュリティ機能を有しないことを検出したとき、上記セキュリティ機能の処理を停止し、上記第1の電子機器の通常動作を開始させることを特徴とする請求項8記載の電子機器のためのセキュリティシステム。

[10] 機器制御ラインを介して接続された、第1の電子機器と第2の電子機器を含む複数の電子機器のためのセキュリティシステムに設けられた第1の電子機器であって、

上記第2の電子機器は、パスワードを予め格納した第2の記憶手段を備え、

上記第1の電子機器は、

パスワードを予め格納した第1の記憶手段と、

上記第1の電子機器の起動時に、上記第2の電子機器に対して上記第2の記憶手段に格納されたパスワードを送信するように要求し、上記第2の電子機器からのパスワードを受信し、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、一致したとき、上記第1の電子機器の動作を開始させるようにセキュリティ機能を実行する制御手段とを備えたことを特徴とするセキュリティシステムのための電子機器。

[11] 上記制御手段は、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき、上記第1の電子機器の動作を停止させるようにセキュリティ機能を実行することを特徴とする請求項10記載のセキュリティシステムのための電子機器。

[12] 上記第1の電子機器は、ユーザーに対するメッセージを表示する表示手段と、パスワードを入力するための入力手段とをさらに備え、

上記制御手段は、上記受信されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき、ユーザーに対してパスワードの入力を要求するように上記表示手段に表示し、上記ユーザーにより上記入力手段を用いて入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、一致したとき上記第1の電子機器の動作を開始させることを特徴とする請求項10記載のセキュリティシステムのための電子機器。

[13] 上記制御手段は、上記ユーザーにより入力されたパスワードを、上記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき上記第1の電子機器の動作を停止させることを特徴とする請求項12記載のセキュリティシステムのための電子機器。

[14] 上記制御手段は、上記ユーザーにより所定の複数回入力されたパスワードを、上

記第1の記憶手段に格納されたパスワードと比較して、不一致であるとき上記第1の電子機器の動作を停止させることを特徴とする請求項12記載のセキュリティシステムのための電子機器。

[15] 上記第1の電子機器は、上記パスワードとは別の特別パスワードを予め格納した第3の記憶手段をさらに備え、

上記制御手段は、上記入力されたパスワードを、上記第3の記憶手段に格納された特別パスワードと比較して、一致したとき、上記第1の電子機器の動作を開始させることを特徴とする請求項12乃至14のうちのいずれか1つに記載のセキュリティシステムのための電子機器。

[16] 上記第1の電子機器は、

上記第1の電子機器に上記第2の電子機器が上記機器制御ラインを介して接続されているか否かを検出する第1の検出手段と、

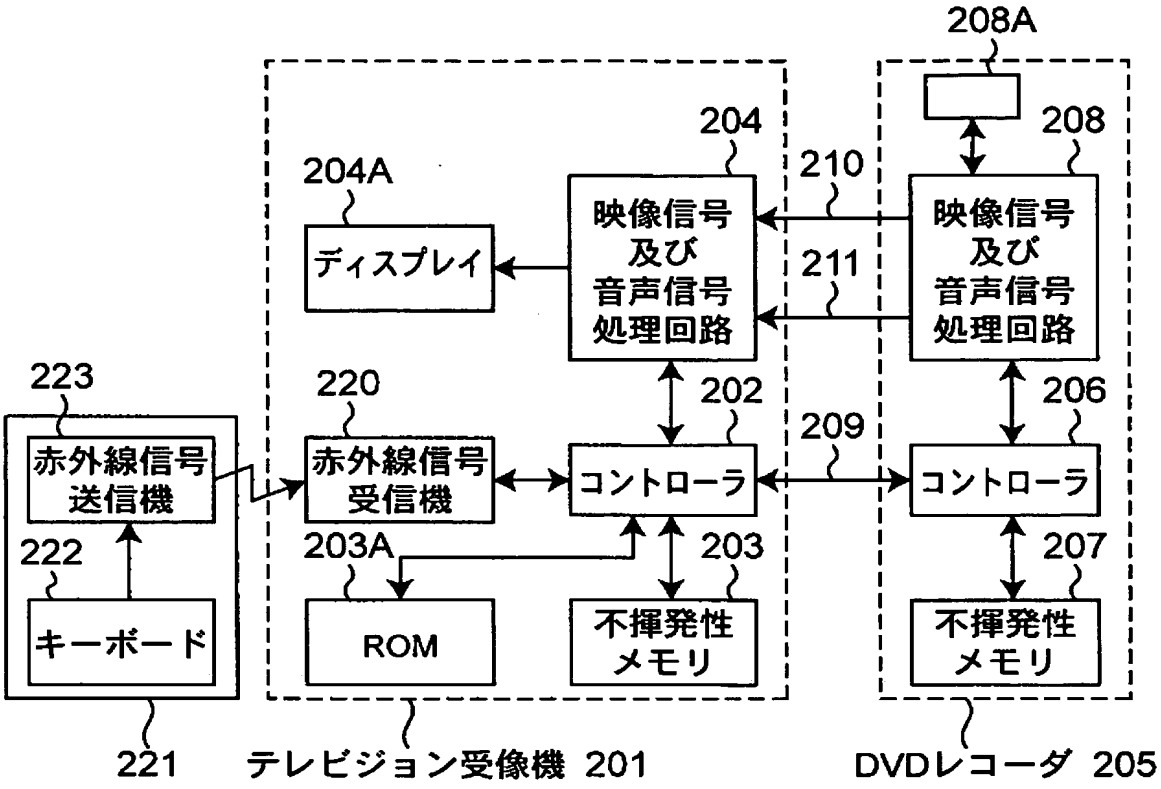
上記第1の検出手段により上記第1の電子機器に上記第2の電子機器が接続されていることを検出したとき、上記機器制御ラインの制御信号を用いて、上記第2の電子機器がセキュリティ機能を有するか否かを検出する第2の検出手段とをさらに備え、

上記制御手段は、上記第1の電子機器の動作中において上記第1の検出手段と上記第2の検出手段の処理を実行することを特徴とする請求項10乃至15のうちのいずれか1つに記載のセキュリティシステムのための電子機器。

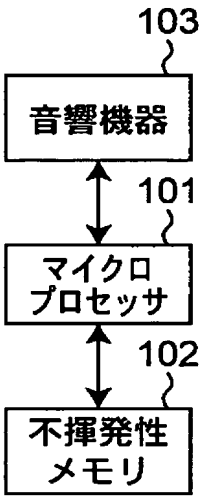
[17] 上記制御手段は、上記第1の検出手段により上記第1の電子機器に上記第2の電子機器が接続されていないことを検出したとき、上記セキュリティ機能の処理を停止し、上記第1の電子機器の通常動作を開始させることを特徴とする請求項16記載のセキュリティシステムのための電子機器。

[18] 上記制御手段は、上記第2の検出手段により上記第2の電子機器が上記セキュリティ機能を有しないことを検出したとき、上記セキュリティ機能の処理を停止し、上記第1の電子機器の通常動作を開始させることを特徴とする請求項17記載のセキュリティシステムのための電子機器。

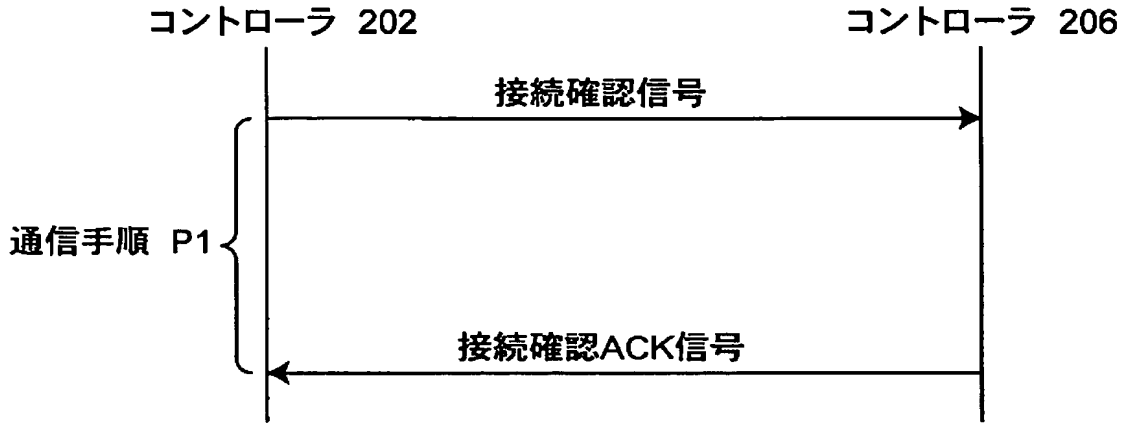
[図1]


208A
204
208
210
204A
映像信号
及び
音声信号
処理回路
映像信号
及び
音声信号
処理回路
ディスプレイ
211
223
220
202
206
209
赤外線信号
送信機
赤外線信号
受信機
コントローラ
コントローラ
222
203A
203
207
キーボード
ROM
不揮発性
メモリ
不揮発性
メモリ
221
テレビジョン受像機 201
DVDレコーダ 205

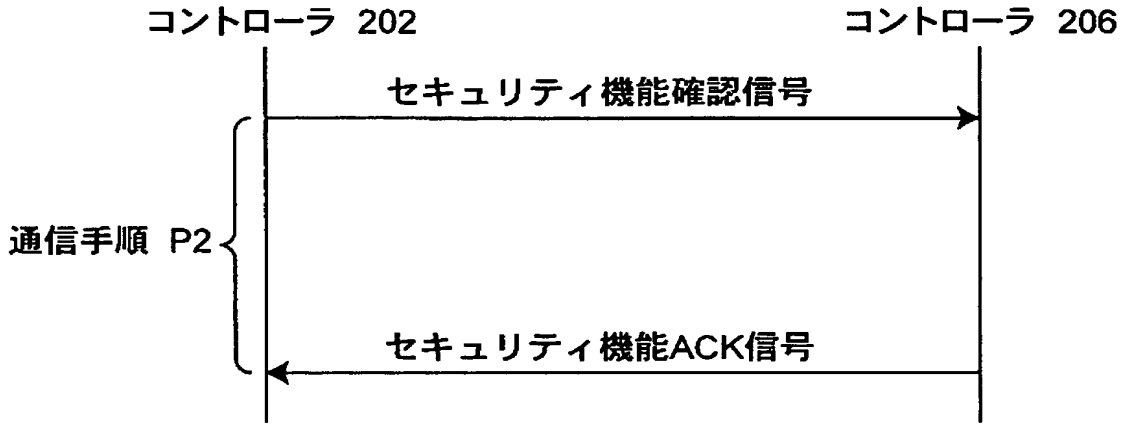
[図2]


103
音響機器
101
マイクロ
プロセッサ
102
不揮発性
メモリ

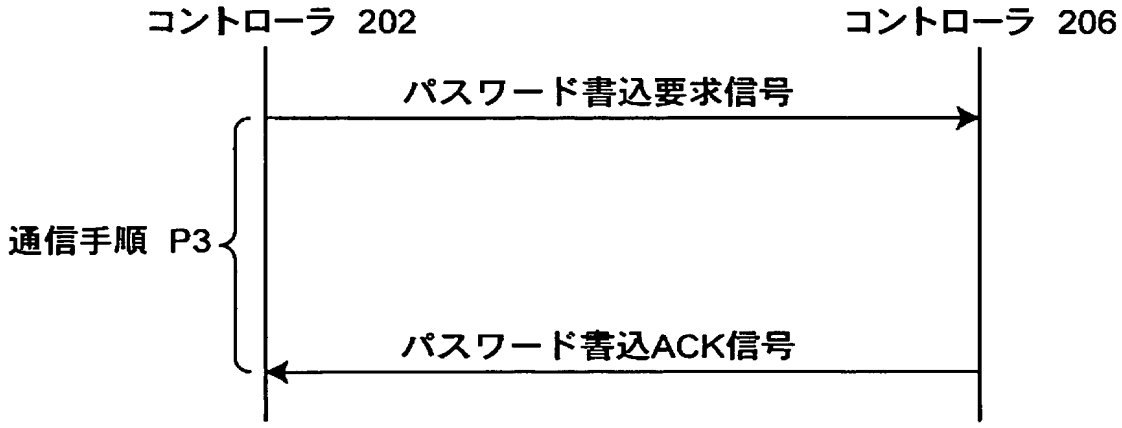
[図3]


コントローラ 202
コントローラ 206
接続確認信号
通信手順 P1
接続確認ACK信号

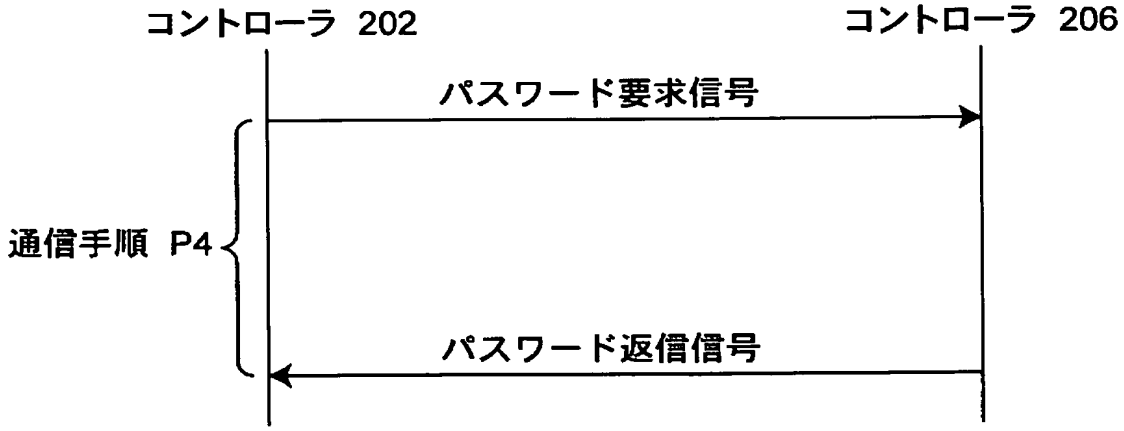
[図4]


コントローラ 202
コントローラ 206
セキュリティ機能確認信号
通信手順 P2
セキュリティ機能ACK信号

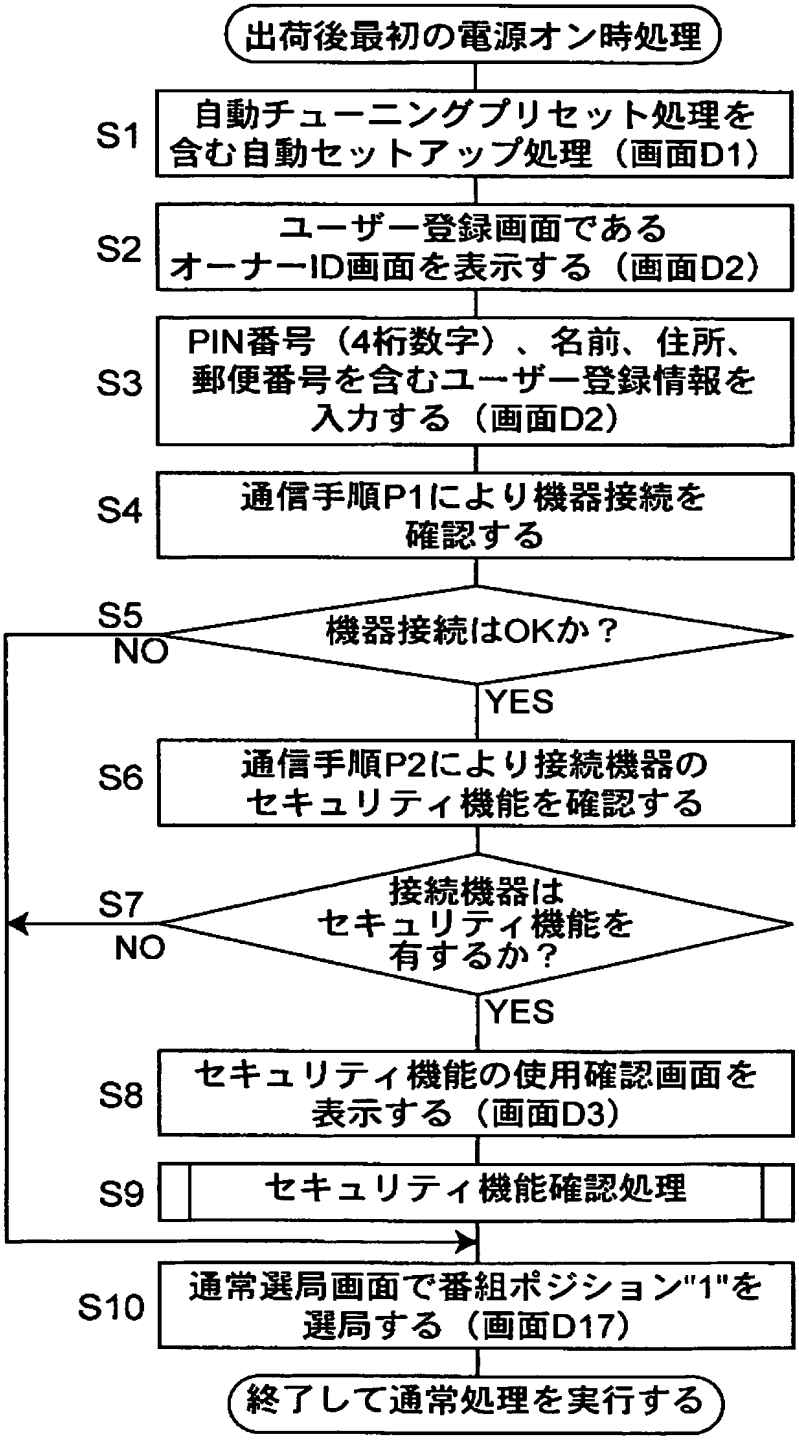
[図5]


コントローラ 202
コントローラ 206
パスワード書込要求信号
通信手順 P3
パスワード書込ACK信号

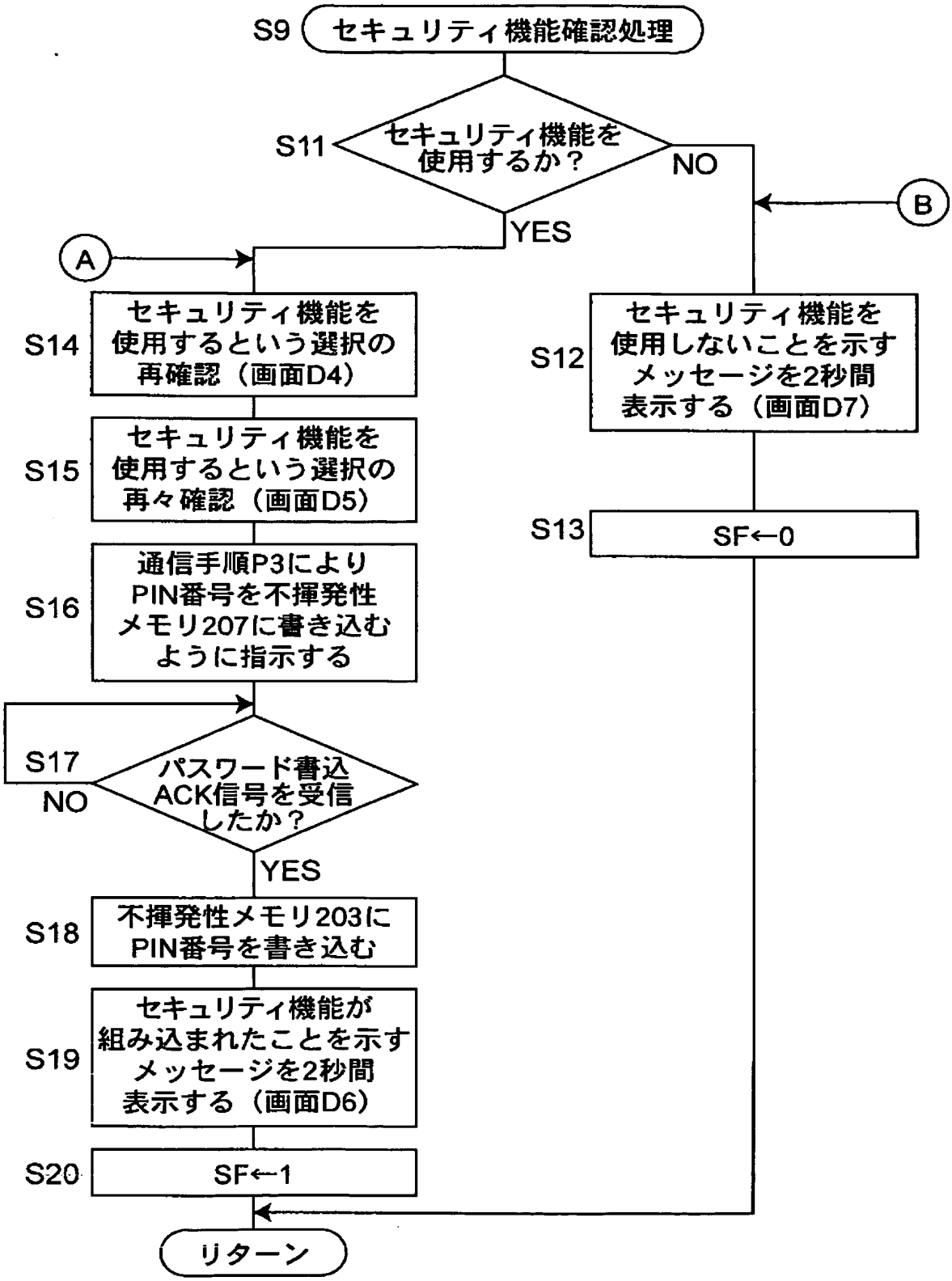
[図6]



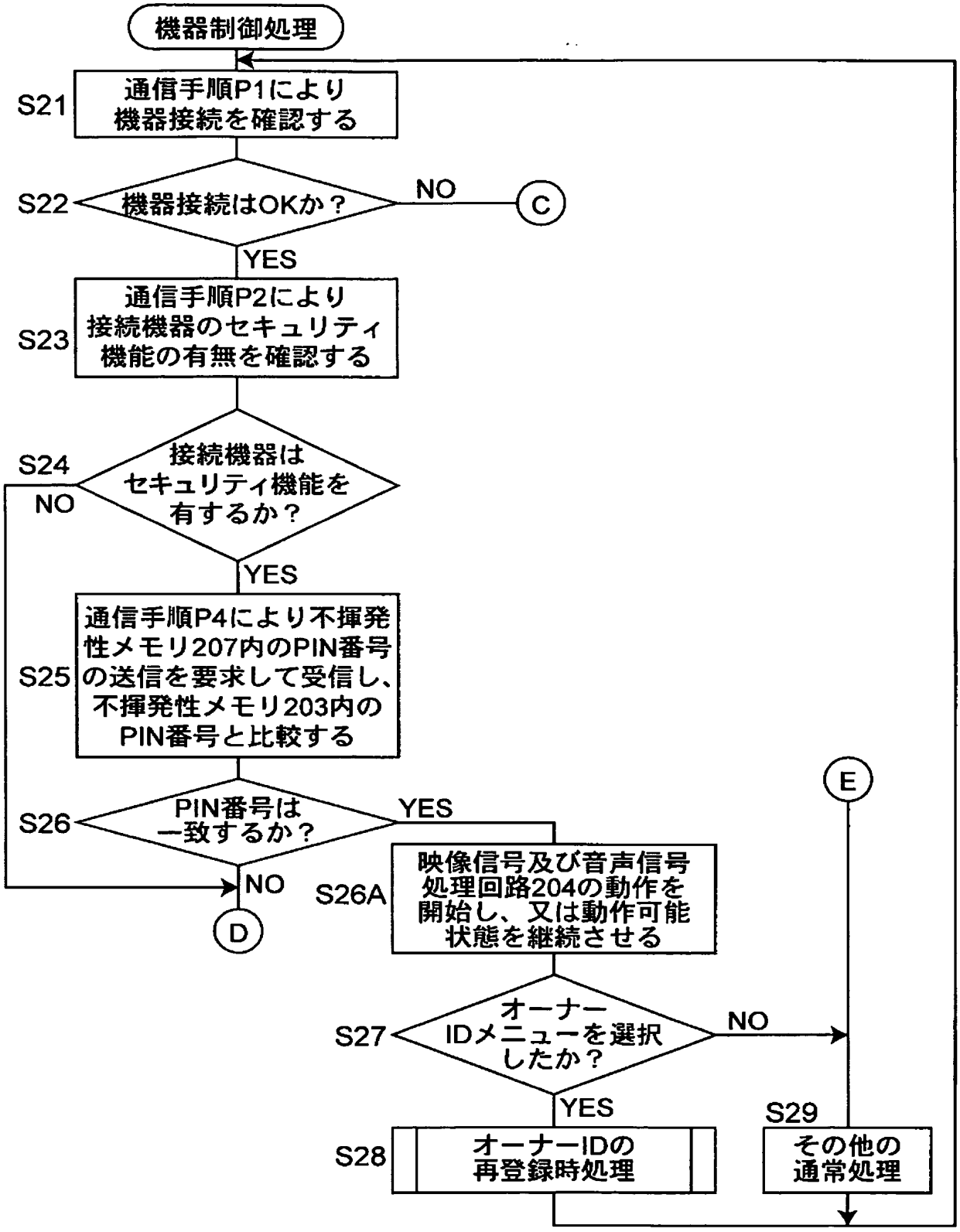
[図7]


出荷後最初の電源オン時処理
S1
自動チューニングプリセット処理を含む自動セットアップ処理（画面D1）
S2
ユーザー登録画面であるオーナーID画面を表示する（画面D2）
S3
PIN番号（4桁数字）、名前、住所、郵便番号を含むユーザー登録情報を入力する（画面D2）
S4
通信手順P1により機器接続を確認する
S5
機器接続はOKか？
NO
YES
S6
通信手順P2により接続機器のセキュリティ機能を確認する
S7
接続機器はセキュリティ機能を有するか？
NO
YES
S8
セキュリティ機能の使用確認画面を表示する（画面D3）
S9
セキュリティ機能確認処理
S10
通常選局画面で番組ポジション"1"を選局する（画面D17）
終了して通常処理を実行する

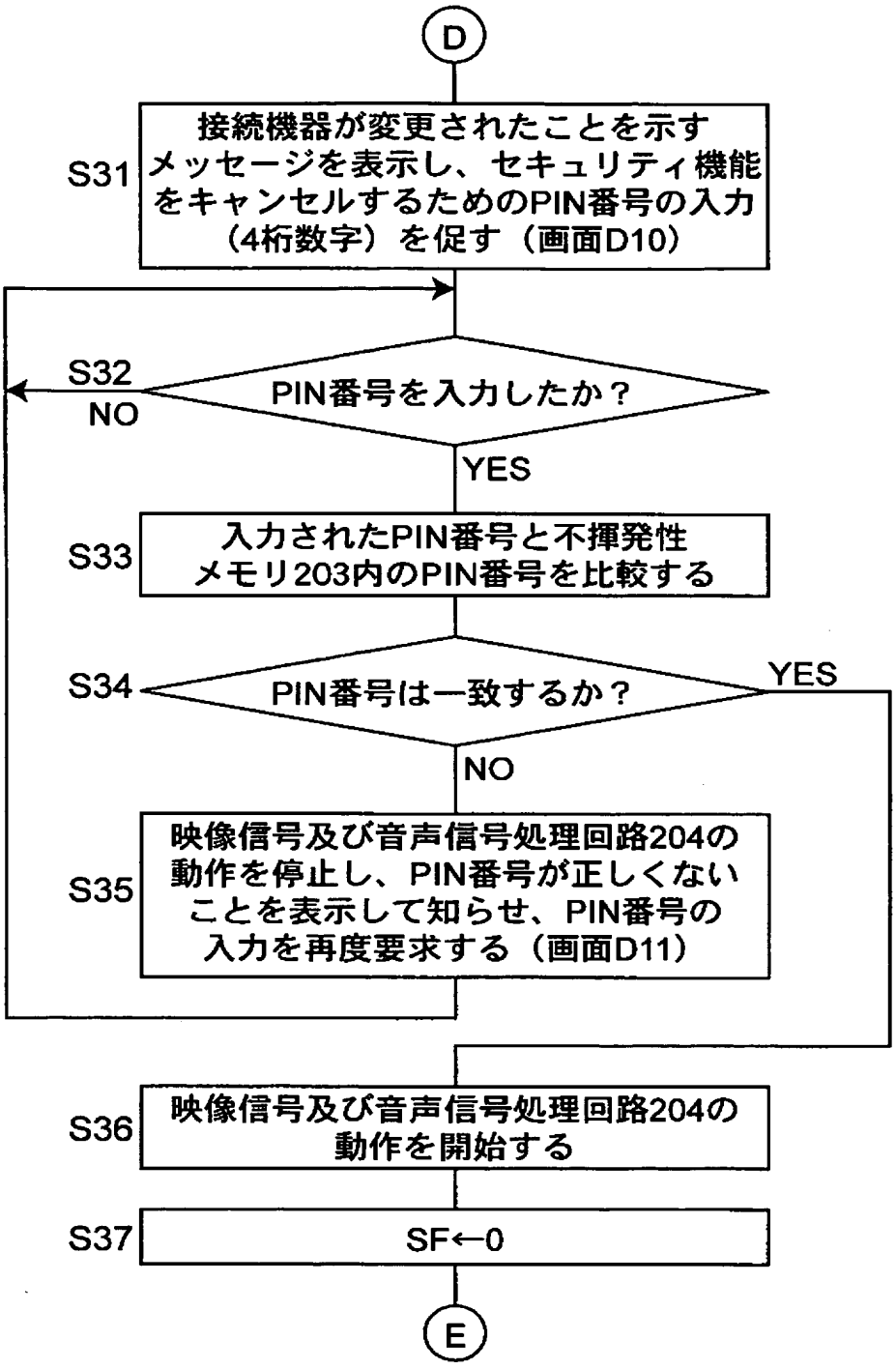
[図8]


S9
セキュリティ機能確認処理
S11
セキュリティ機能を使用するか？
NO
YES
B
A
S14
セキュリティ機能を使用するという選択の再確認（画面D4）
S15
セキュリティ機能を使用するという選択の再々確認（画面D5）
S16
通信手順P3によりPIN番号を不揮発性メモリ207に書き込むように指示する
S17
NO
パスワード書込ACK信号を受信したか？
YES
S18
不揮発性メモリ203にPIN番号を書き込む
S19
セキュリティ機能が組み込まれたことを示すメッセージを2秒間表示する（画面D6）
S20
SF←1
S12
セキュリティ機能を使用しないことを示すメッセージを2秒間表示する（画面D7）
S13
SF←0
リターン

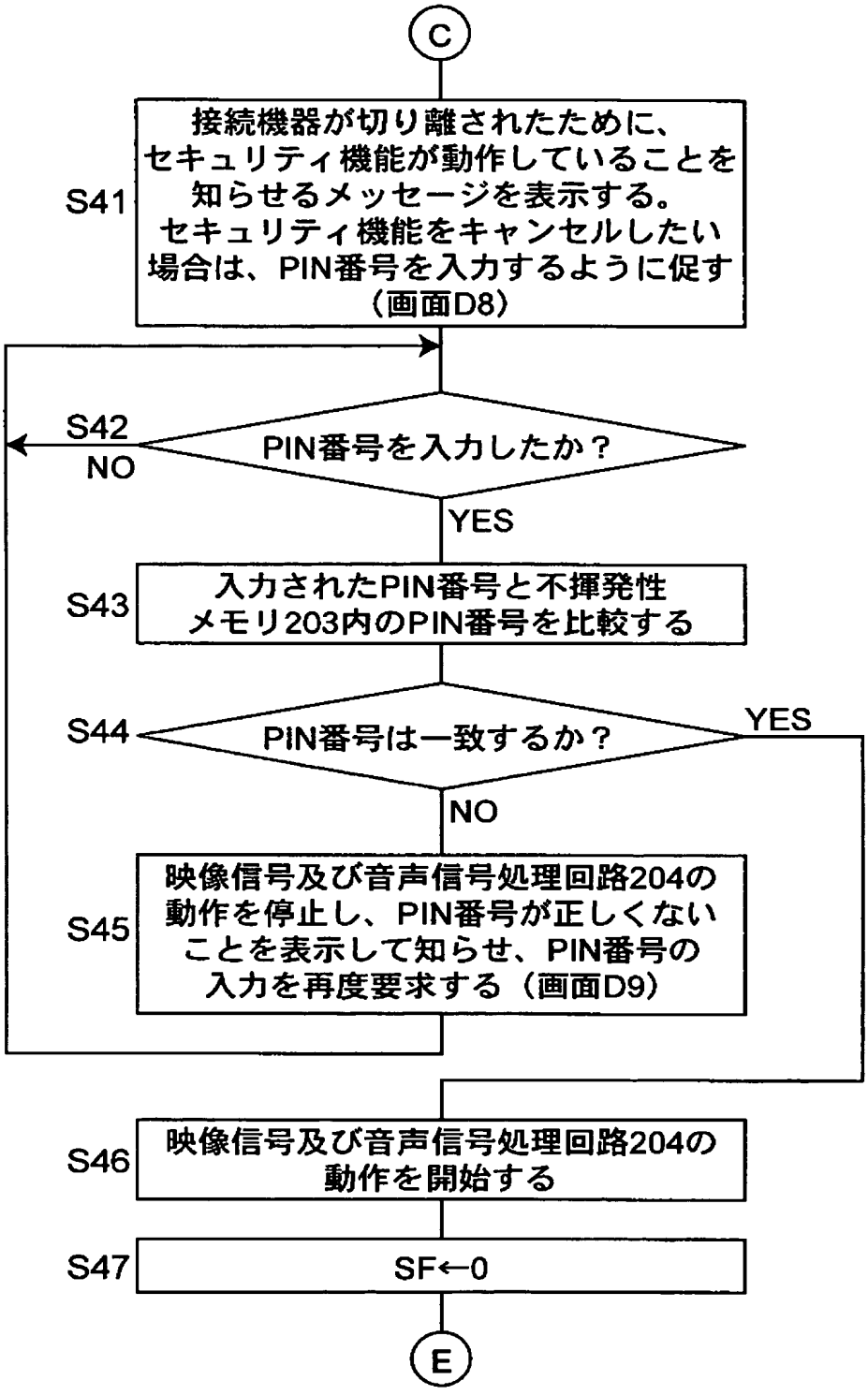
[図9]


機器制御処理
S21
通信手順P1により
機器接続を確認する
S22
機器接続はOKか？
NO
C
YES
S23
通信手順P2により
接続機器のセキュリティ
機能の有無を確認する
S24
接続機器は
セキュリティ機能を
有するか？
NO
YES
S25
通信手順P4により不揮発
性メモリ207内のPIN番号
の送信を要求して受信し、
不揮発性メモリ203内の
PIN番号と比較する
S26
PIN番号は
一致するか？
YES
NO
D
S26A
映像信号及び音声信号
処理回路204の動作を
開始し、又は動作可能
状態を継続させる
E
S27
オーナー
IDメニューを選択
したか？
NO
YES
S28
オーナーIDの
再登録時処理
S29
その他の
通常処理

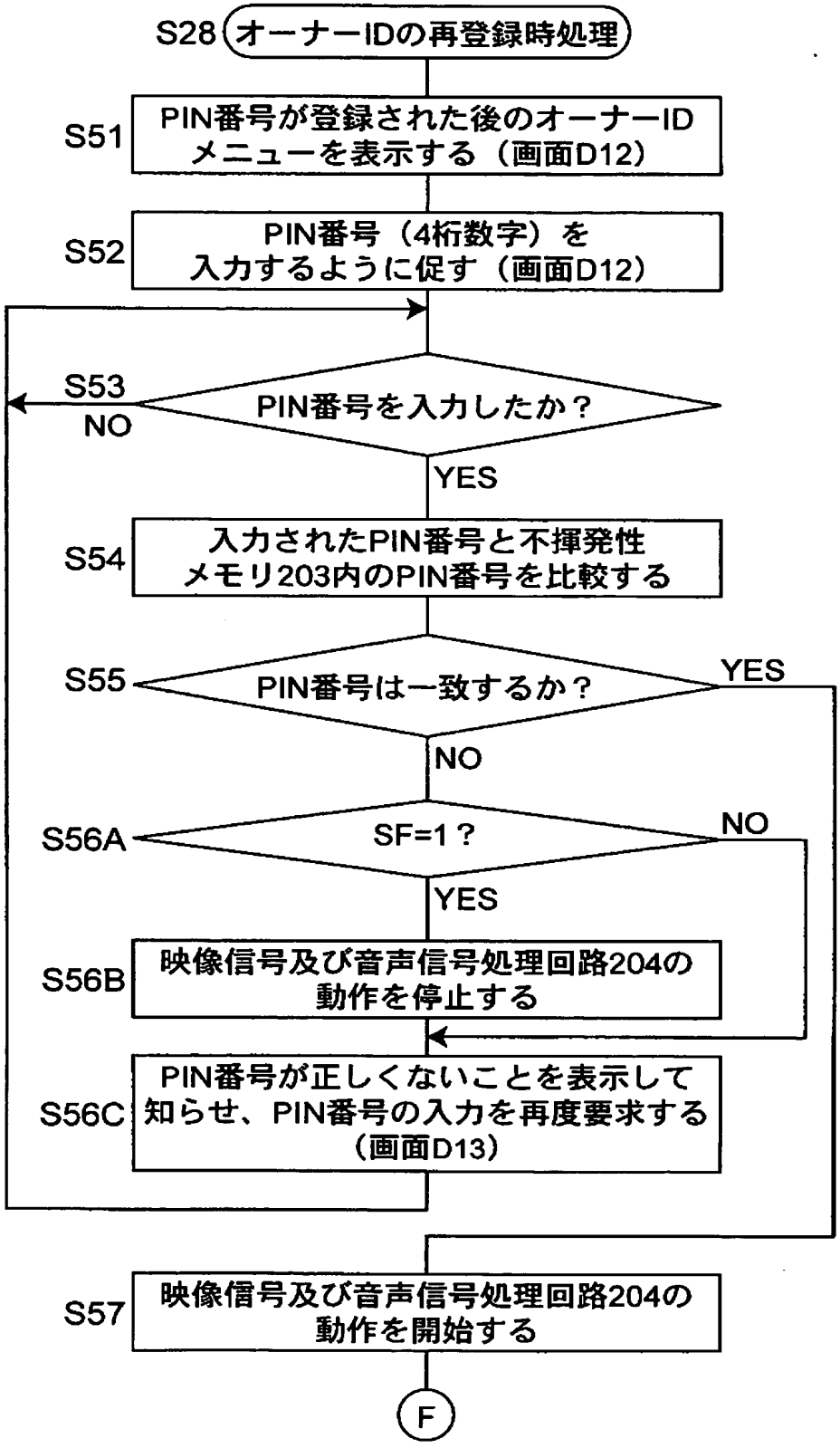
[図10]


D
S31
接続機器が変更されたことを示すメッセージを表示し、セキュリティ機能をキャンセルするためのPIN番号の入力（4桁数字）を促す（画面D10）
S32
NO
PIN番号を入力したか？
YES
S33
入力されたPIN番号と不揮発性メモリ203内のPIN番号を比較する
S34
PIN番号は一致するか？
YES
NO
S35
映像信号及び音声信号処理回路204の動作を停止し、PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求する（画面D11）
S36
映像信号及び音声信号処理回路204の動作を開始する
S37
SF←0
E

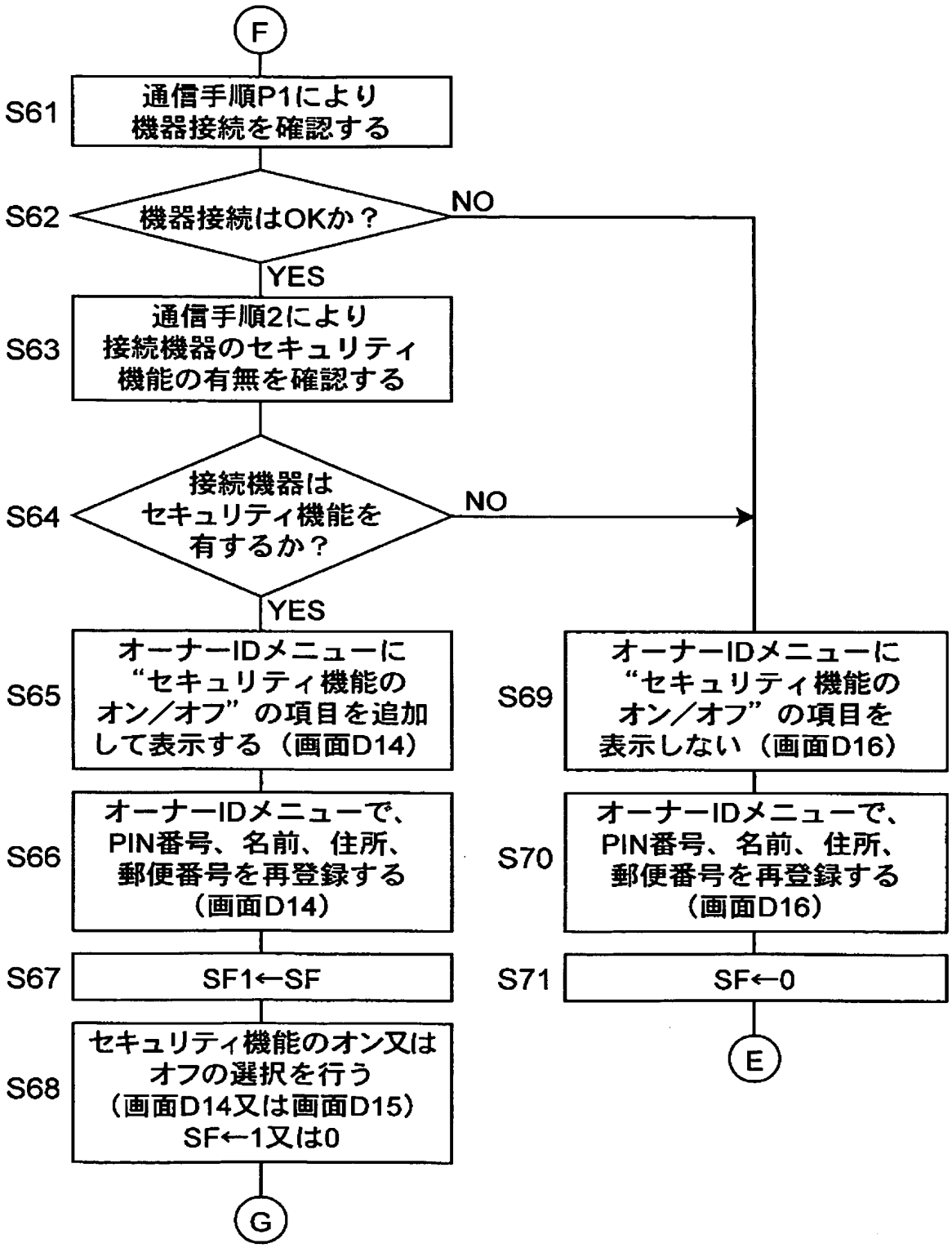
[図11]


C
S41
接続機器が切り離されたために、セキュリティ機能が動作していることを知らせるメッセージを表示する。セキュリティ機能をキャンセルしたい場合は、PIN番号を入力するように促す（画面D8）
S42
PIN番号を入力したか？
NO
YES
S43
入力されたPIN番号と不揮発性メモリ203内のPIN番号を比較する
S44
PIN番号は一致するか？
YES
NO
S45
映像信号及び音声信号処理回路204の動作を停止し、PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求する（画面D9）
S46
映像信号及び音声信号処理回路204の動作を開始する
S47
SF←0
E

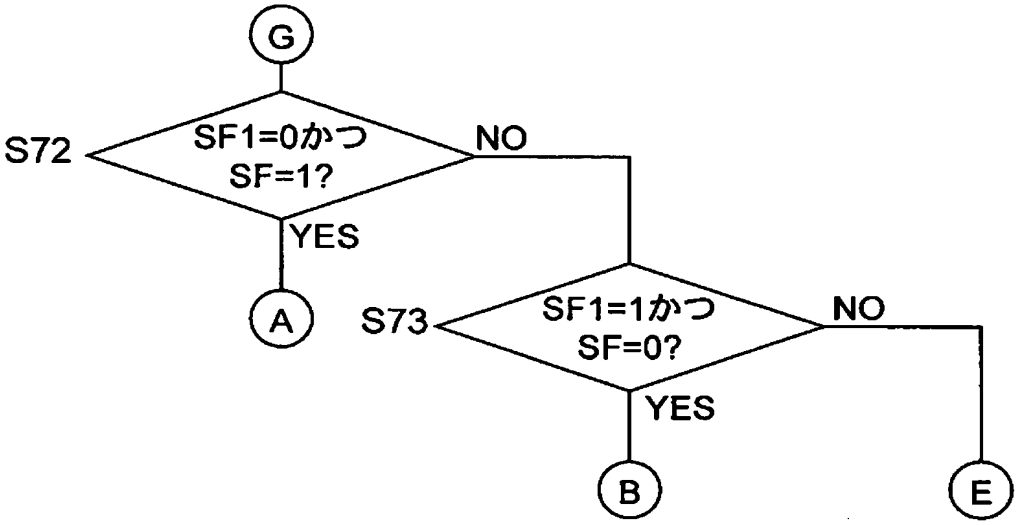
[図12]


S28 オーナーIDの再登録時処理
S51 PIN番号が登録された後のオーナーID メニューを表示する（画面D12）
S52 PIN番号（4桁数字）を 入力するように促す（画面D12）
S53 PIN番号を入力したか？
NO
YES
S54 入力されたPIN番号と不揮発性 メモリ203内のPIN番号を比較する
S55 PIN番号は一致するか？
YES
NO
S56A SF=1？
NO
YES
S56B 映像信号及び音声信号処理回路204の 動作を停止する
S56C PIN番号が正しくないことを表示して 知らせ、PIN番号の入力を再度要求する （画面D13）
S57 映像信号及び音声信号処理回路204の 動作を開始する
F

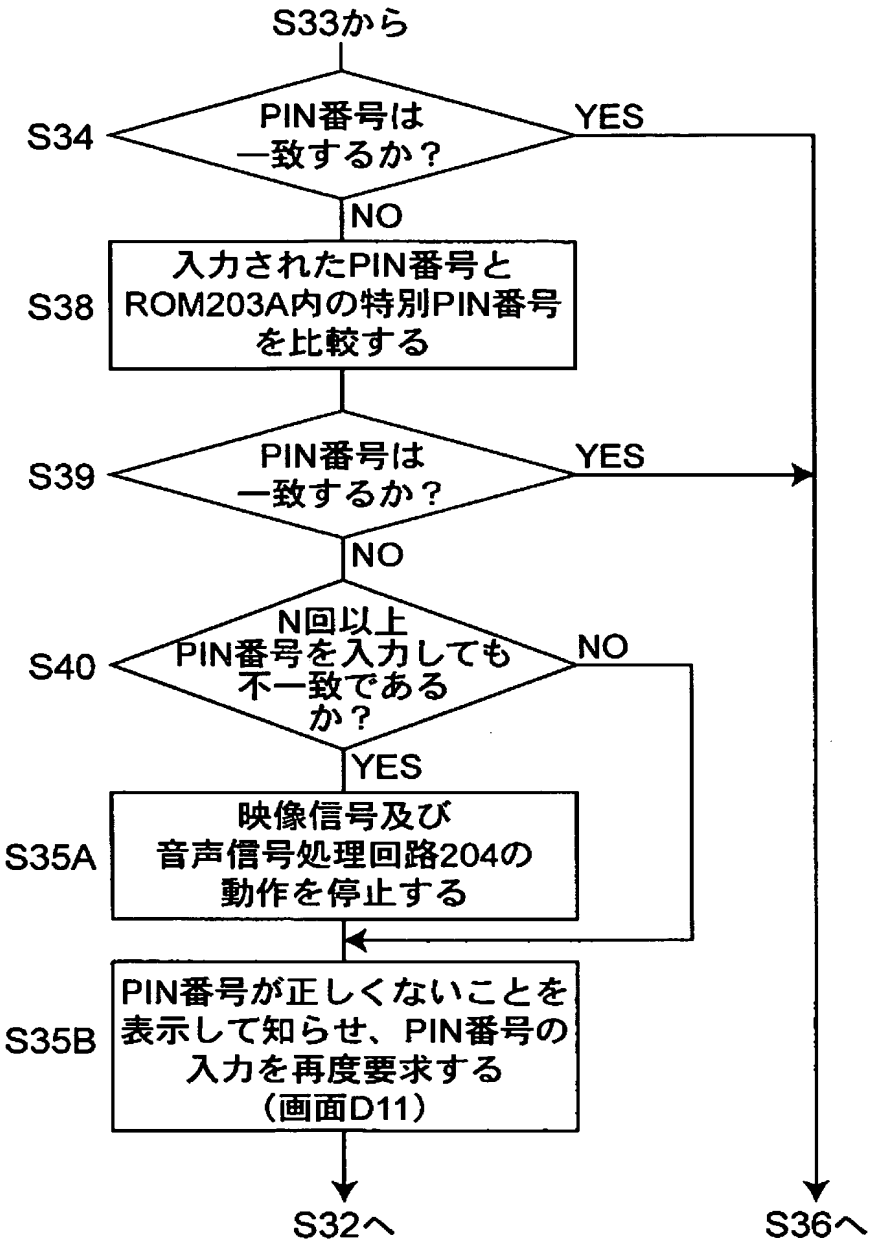
[図13]


F
S61
通信手順P1により
機器接続を確認する
S62
機器接続はOKか？
NO
YES
S63
通信手順2により
接続機器のセキュリティ
機能の有無を確認する
S64
接続機器は
セキュリティ機能を
有するか？
NO
YES
S65
オーナーIDメニューに
“セキュリティ機能の
オン／オフ”の項目を追加
して表示する（画面D14）
S66
オーナーIDメニューで、
PIN番号、名前、住所、
郵便番号を再登録する
（画面D14）
S67
SF1←SF
S68
セキュリティ機能のオン又は
オフの選択を行う
（画面D14又は画面D15）
SF←1又は0
G
S69
オーナーIDメニューに
“セキュリティ機能の
オン／オフ”の項目を
表示しない（画面D16）
S70
オーナーIDメニューで、
PIN番号、名前、住所、
郵便番号を再登録する
（画面D16）
S71
SF←0
E

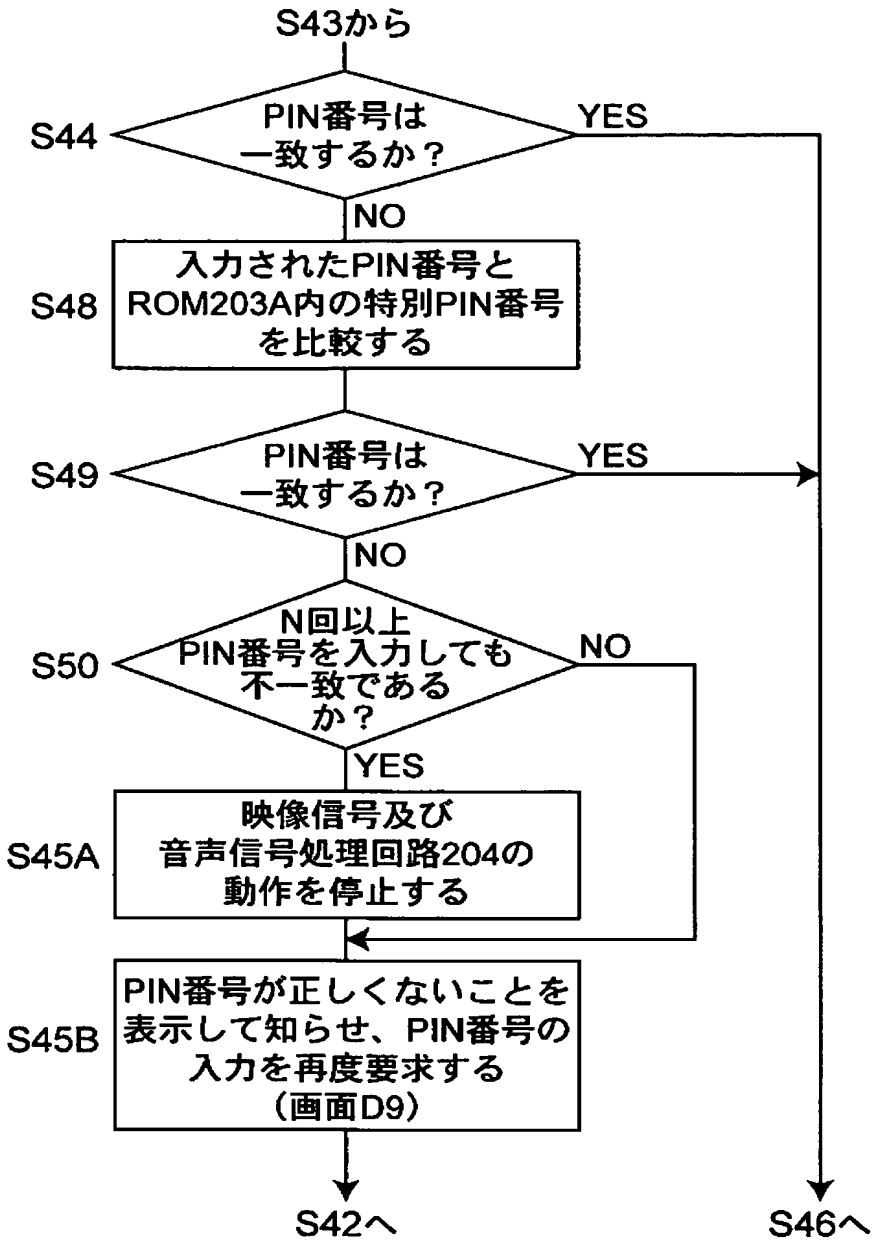
[図14]



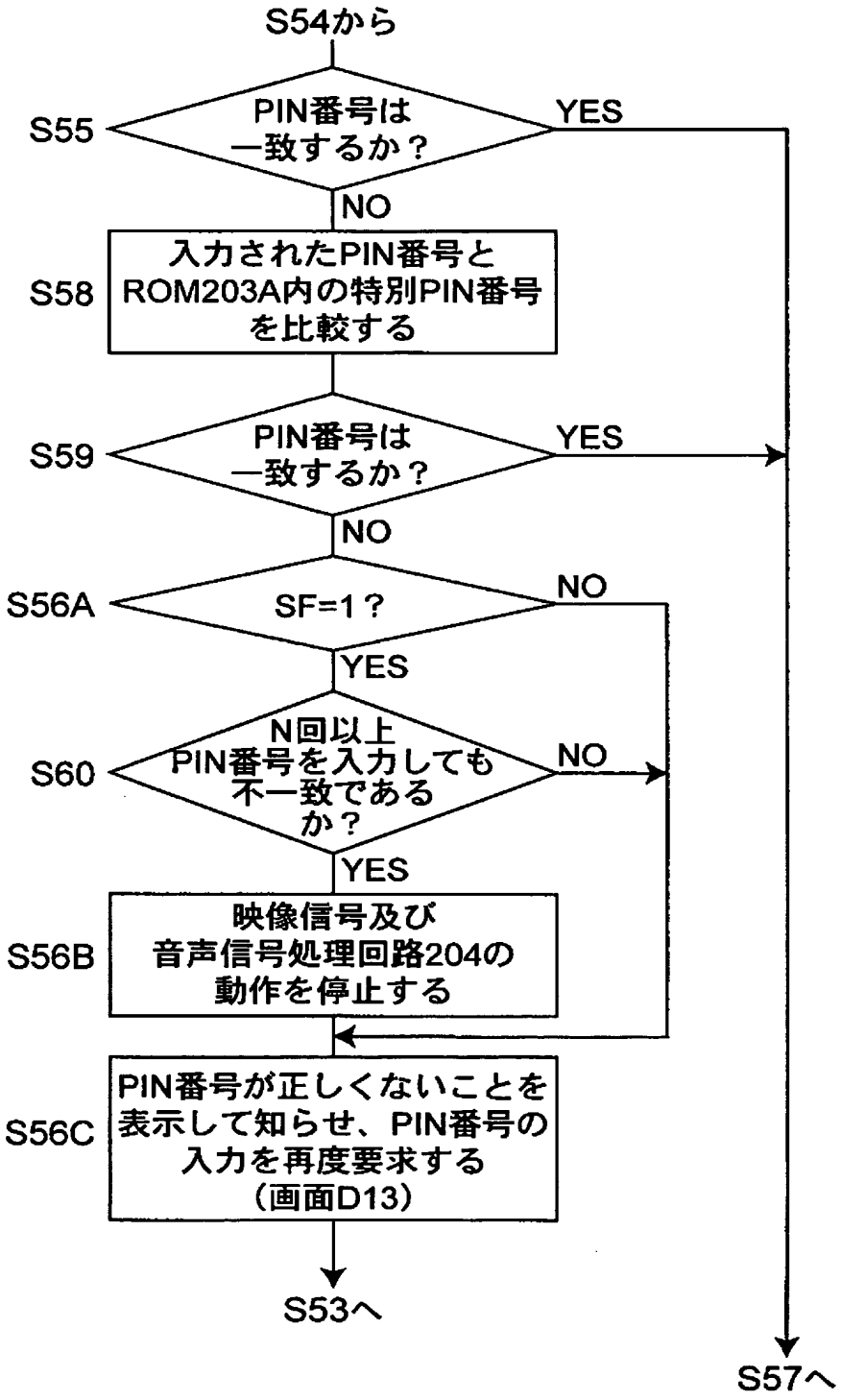
[図15]


S33から
S34
PIN番号は一致するか？
YES
NO
S38
入力されたPIN番号とROM203A内の特別PIN番号を比較する
S39
PIN番号は一致するか？
YES
NO
S40
N回以上PIN番号を入力しても不一致であるか？
NO
YES
S35A
映像信号及び音声信号処理回路204の動作を停止する
S35B
PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求する（画面D11）
S32へ
S36へ

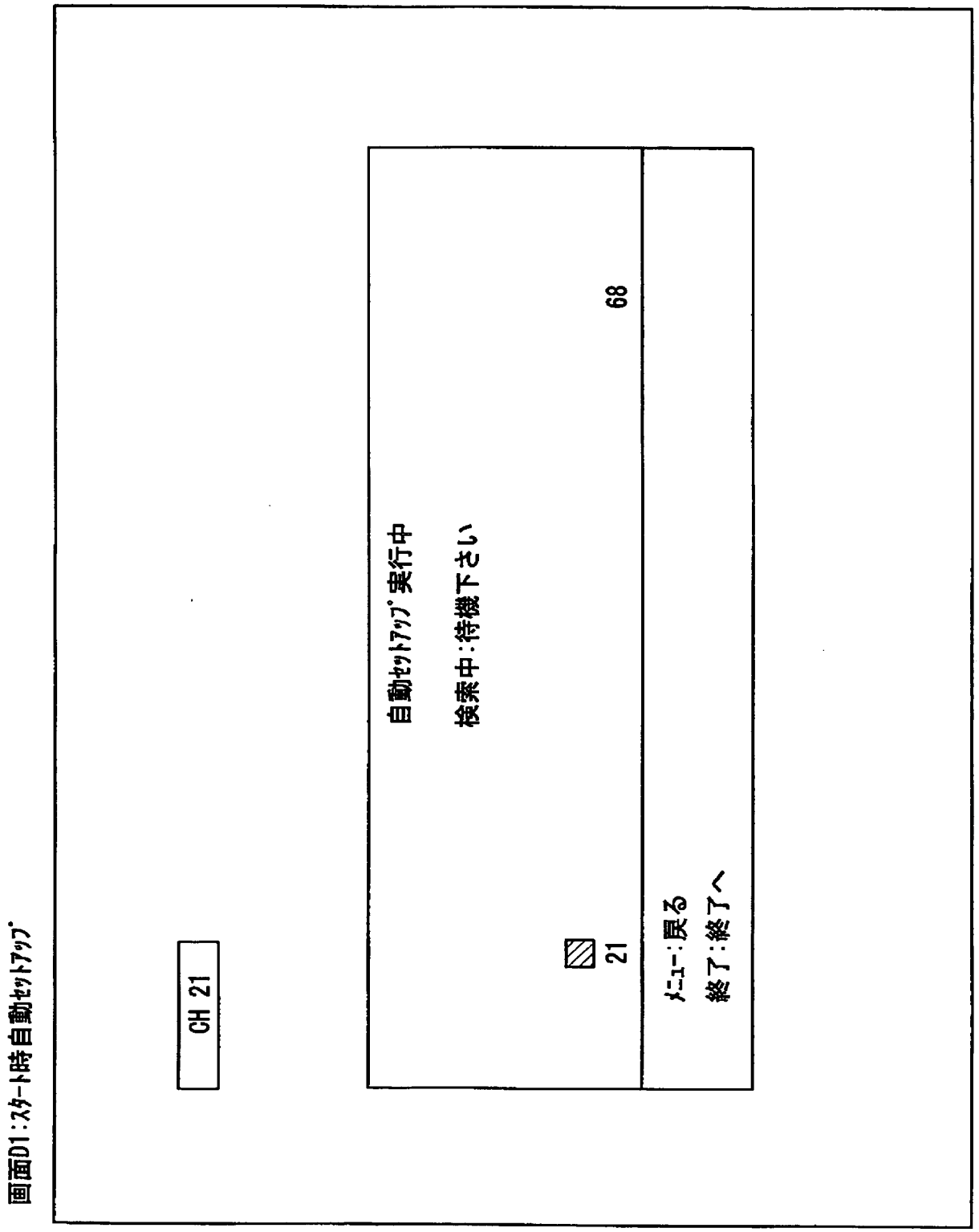
[図16]


S43から
S44
PIN番号は一致するか？
YES
NO
S48
入力されたPIN番号とROM203A内の特別PIN番号を比較する
S49
PIN番号は一致するか？
YES
NO
S50
N回以上PIN番号を入力しても不一致であるか？
NO
YES
S45A
映像信号及び音声信号処理回路204の動作を停止する
S45B
PIN番号が正しくないことを表示して知らせ、PIN番号の入力を再度要求する（画面D9）
S42へ
S46へ

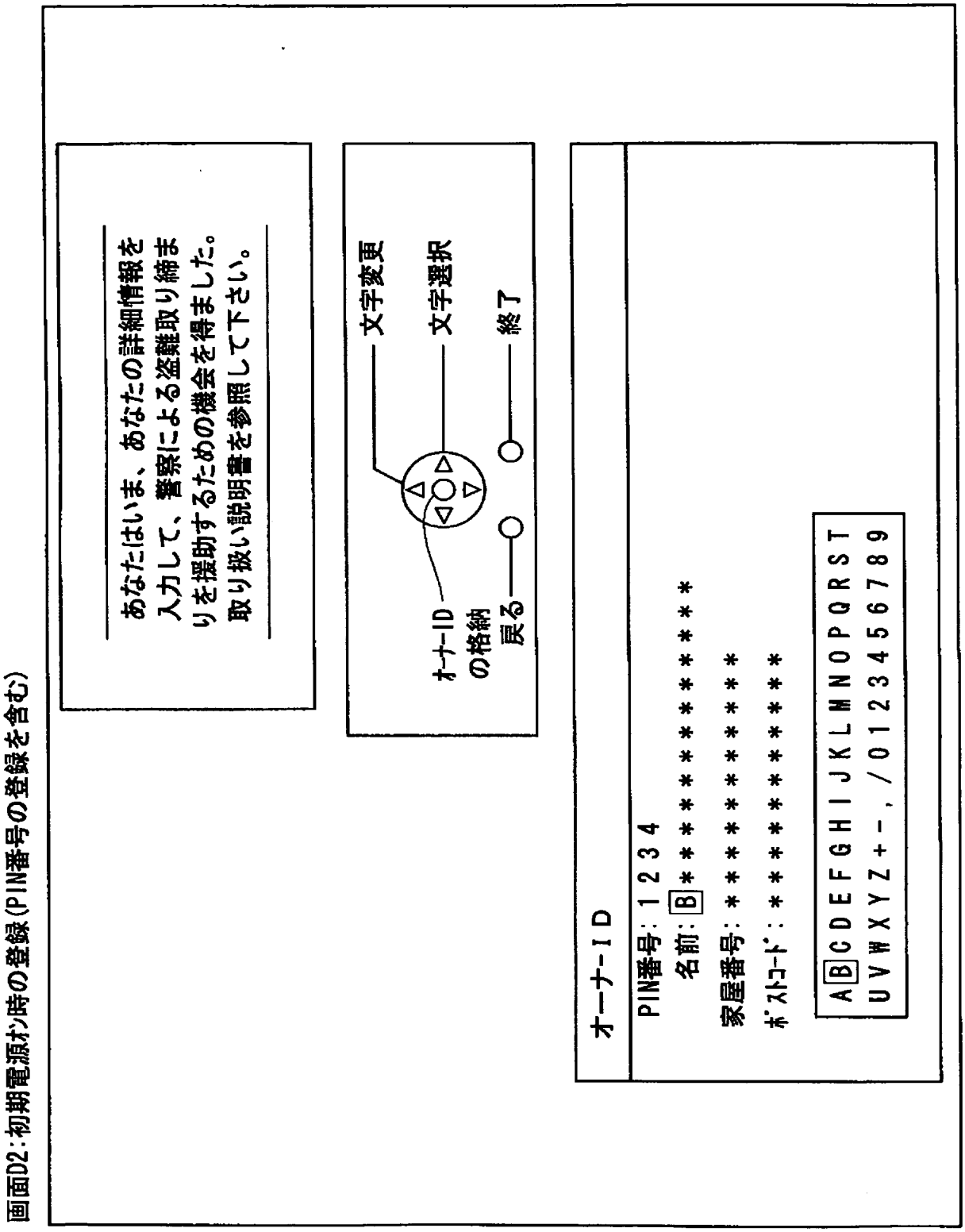
[図17]


S54から
S55
PIN番号は
一致するか？
YES
NO
S58
入力されたPIN番号と
ROM203A内の特別PIN番号
を比較する
S59
PIN番号は
一致するか？
YES
NO
S56A
SF=1？
NO
YES
S60
N回以上
PIN番号を入力しても
不一致である
か？
NO
YES
S56B
映像信号及び
音声信号処理回路204の
動作を停止する
S56C
PIN番号が正しくないことを
表示して知らせ、PIN番号の
入力を再度要求する
（画面D13）
S53へ
S57へ

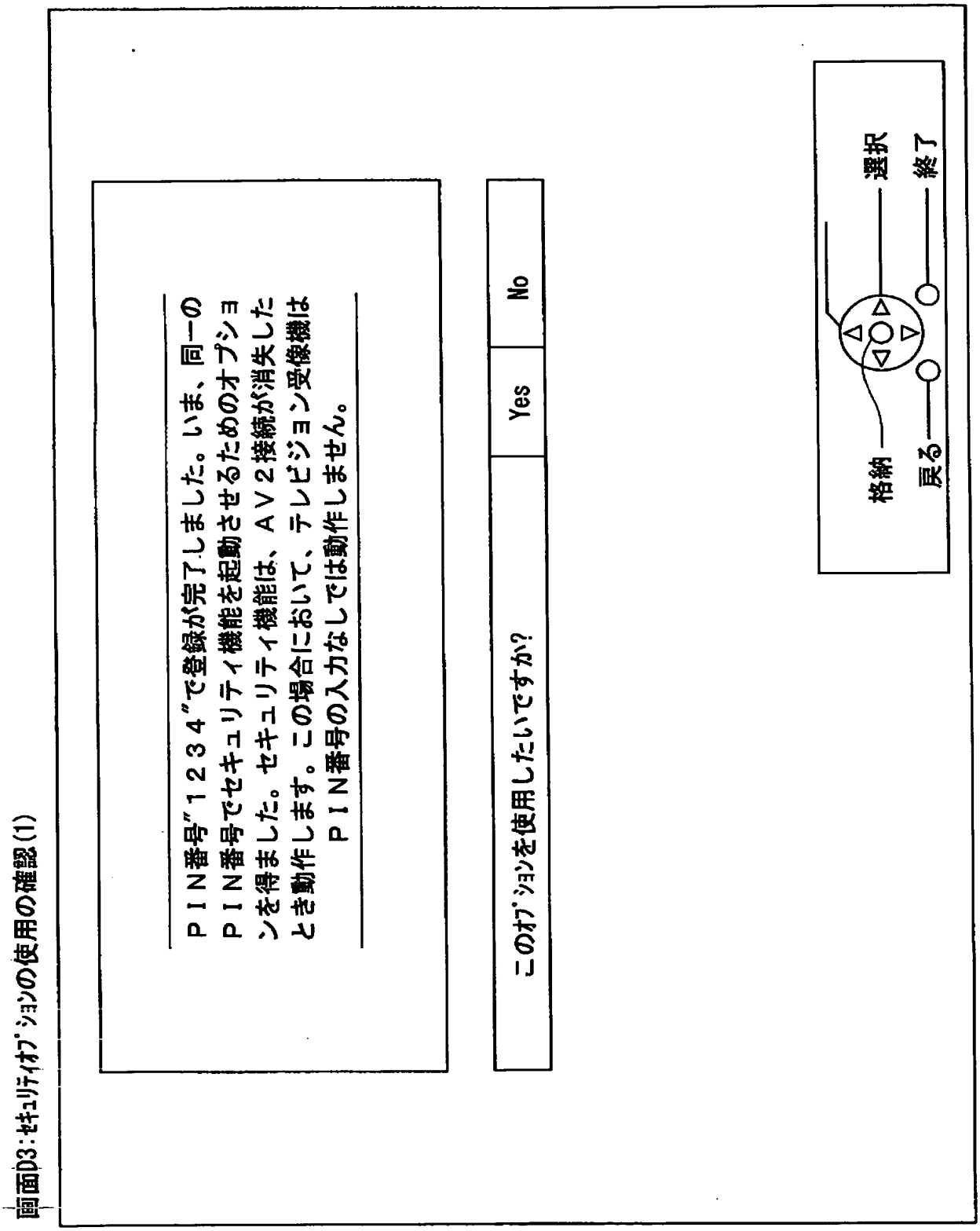
[図18]


画面D1:スタート時自動セットアップ
CH 21
自動セットアップ実行中
検索中:待機下さい
68
21
メニュー:戻る
終了:終了へ

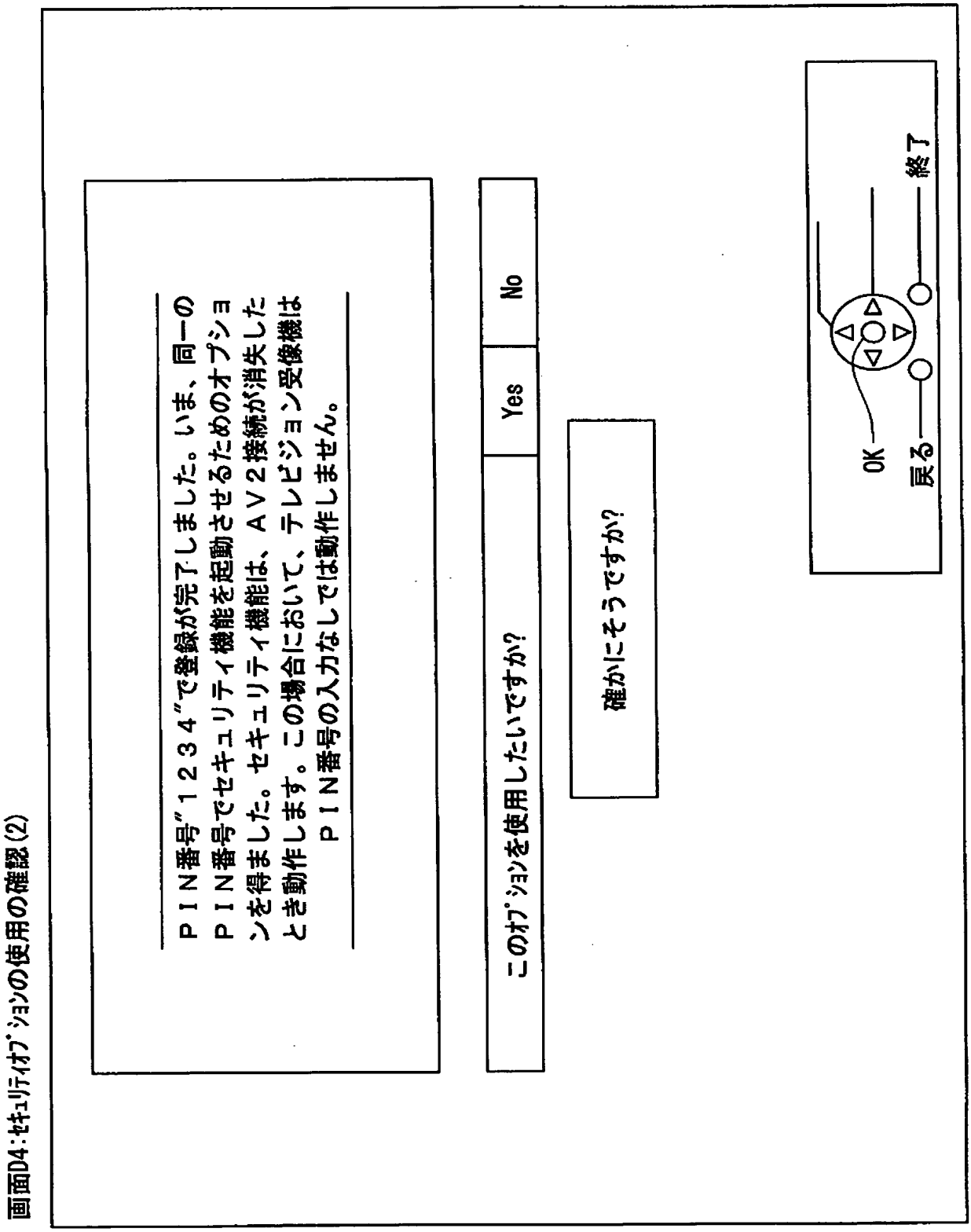
[図19]


画面D2:初期電源ON時の登録(PIN番号の登録を含む)
オーナーID
PIN番号:1234
名前:B**********
家屋番号:**********
ﾎﾟｽﾄｺｰﾄﾞ:**********
ABCDEFGHIJKLMNOPQRST
UVWXYZ+-,/0123456789
オーナーIDの格納
戻る
文字変更
文字選択
終了
あなたはいま、あなたの詳細情報を入力して、警察による盗難取り締まりを援助するための機会を得ました。取り扱い説明書を参照して下さい。

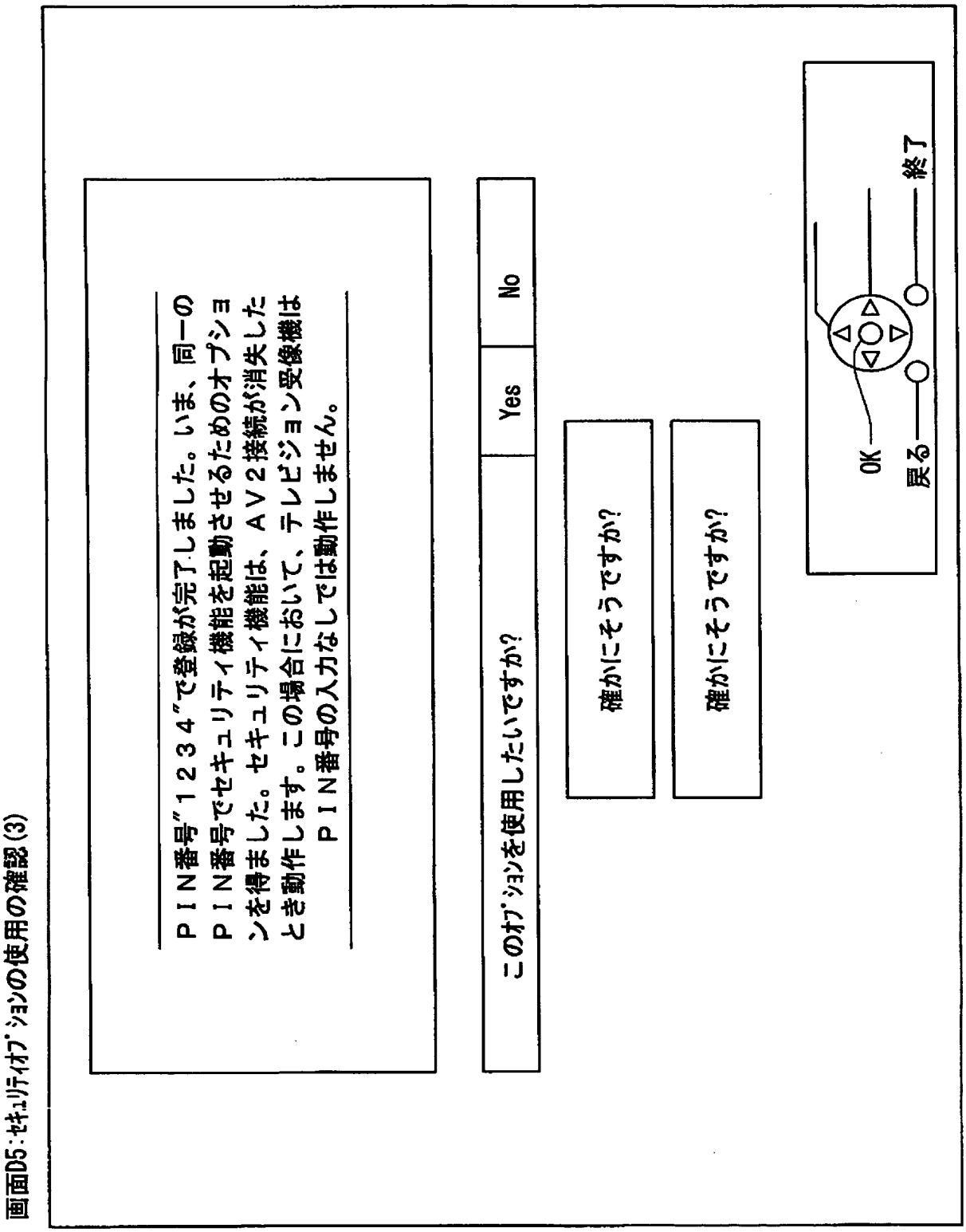
[図20]


画面D3：セキュリティオプションの使用の確認(1)
PIN番号"1234"で登録が完了しました。いま、同一のPIN番号でセキュリティ機能を起動させるためのオプションを得ました。セキュリティ機能は、AV2接続が消失したとき動作します。この場合において、テレビジョン受像機はPIN番号の入力なしでは動作しません。
このオプションを使用したいですか?
Yes
No
選択
終了
格納
戻る

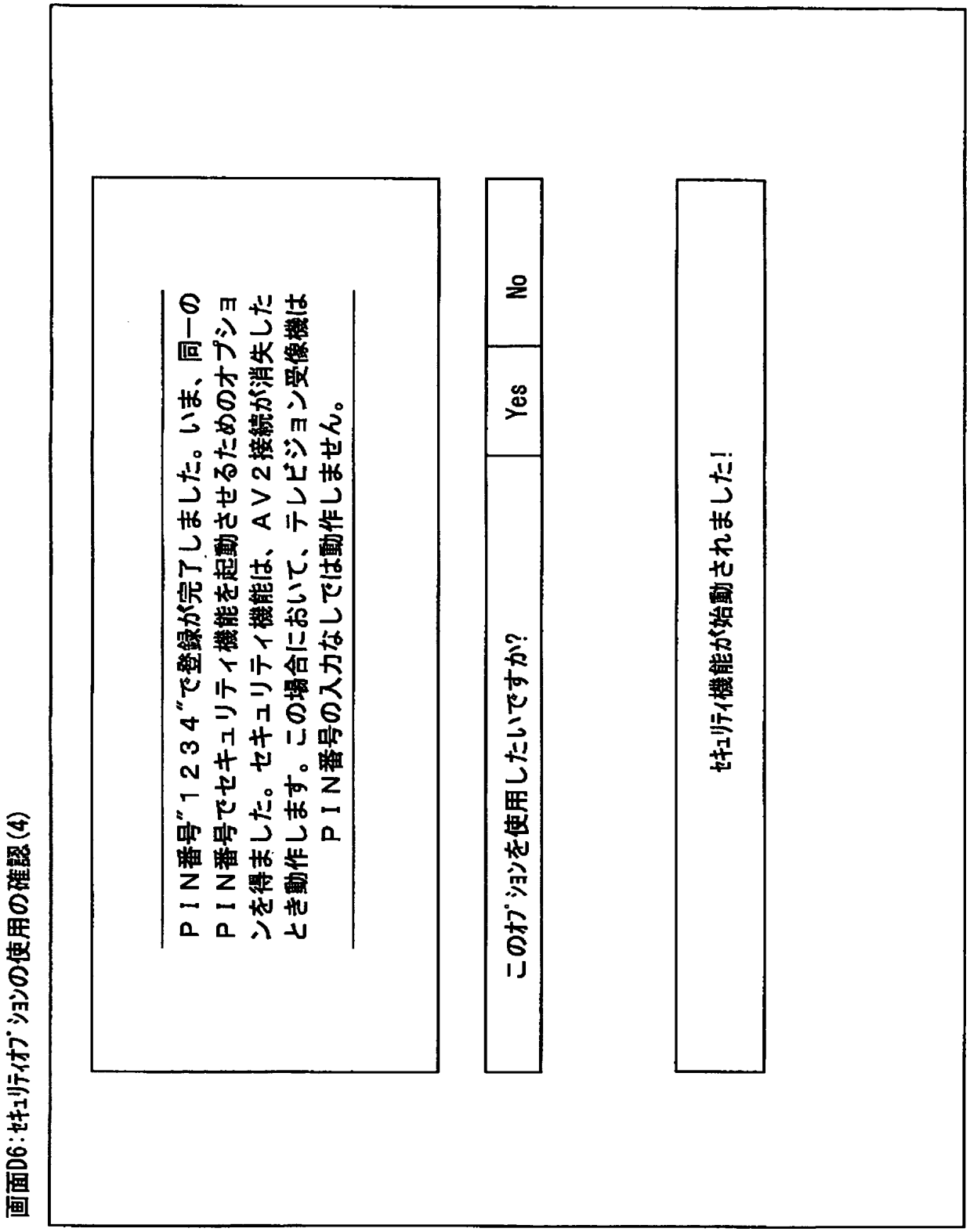
[図21]


画面D4:セキュリティオプションの使用の確認(2)
PIN番号"1234"で登録が完了しました。いま、同一のPIN番号でセキュリティ機能を起動させるためのオプションを得ました。セキュリティ機能は、AV2接続が消失したとき動作します。この場合において、テレビジョン受像機はPIN番号の入力なしでは動作しません。
このオプションを使用したいですか?
Yes
No
確かにそうですか?
OK
戻る
終了

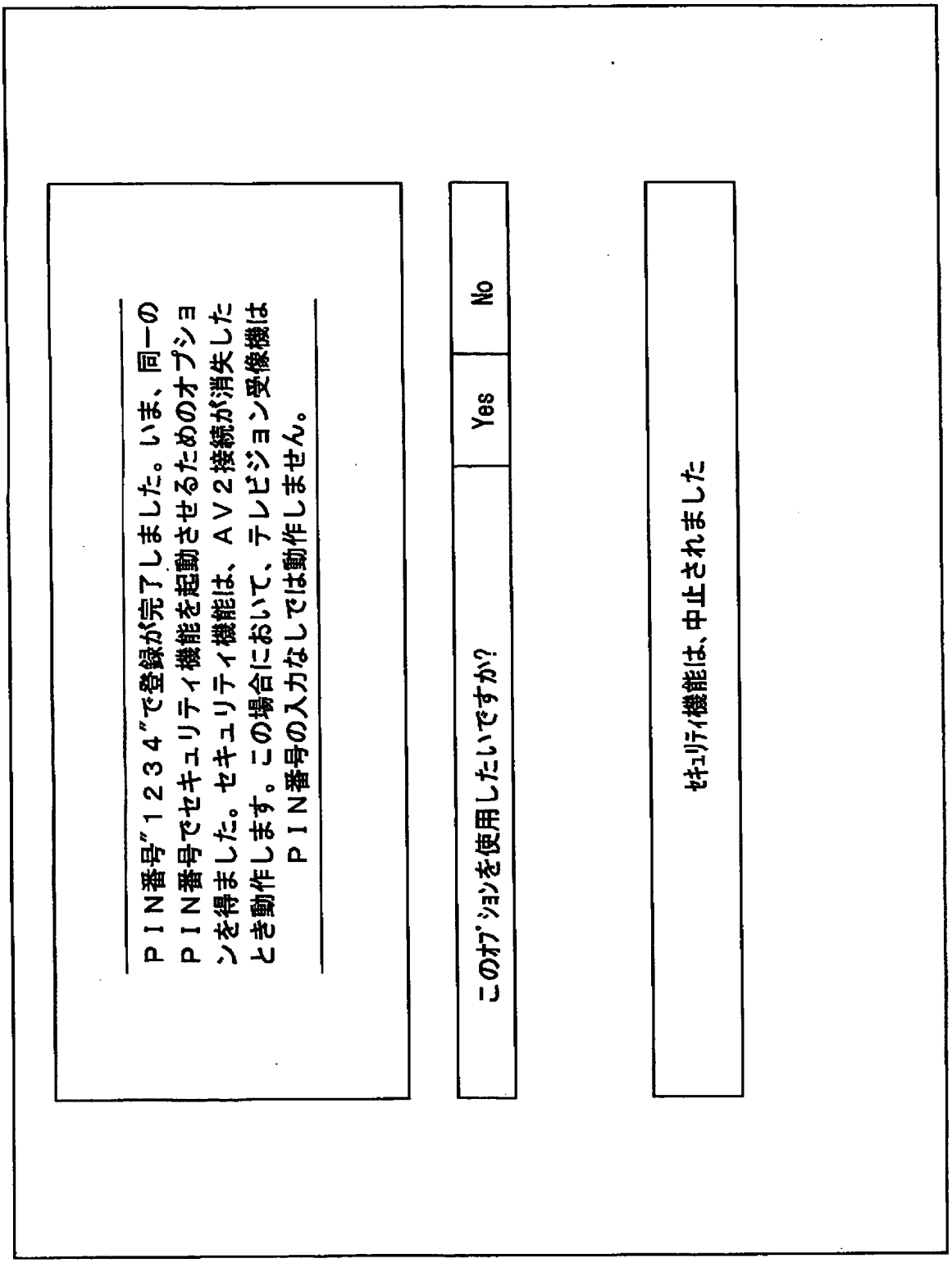
[図22]


画面D5：セキュリティオプションの使用の確認(3)
PIN番号"1234"で登録が完了しました。いま、同一のPIN番号でセキュリティ機能を起動させるためのオプションを得ました。セキュリティ機能は、AV2接続が消失したとき動作します。この場合において、テレビジョン受像機はPIN番号の入力なしでは動作しません。
このオプションを使用したいですか?
Yes
No
確かにそうですか?
確かにそうですか?
OK
戻る
終了

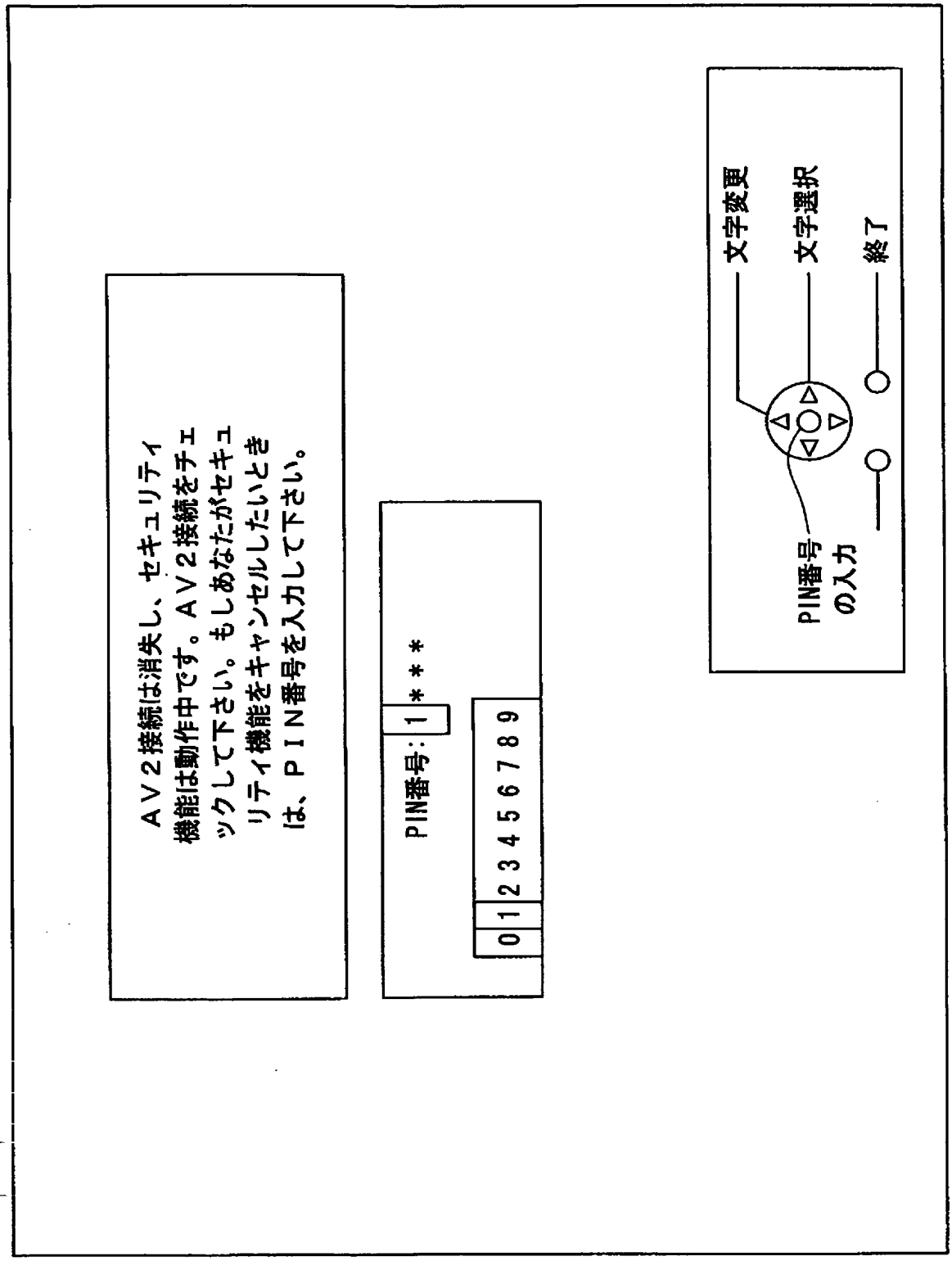
[図23]


画面D6：セキュリティオプションの使用の確認(4)
PIN番号"1234"で登録が完了しました。いま、同一のPIN番号でセキュリティ機能を起動させるためのオプションを得ました。セキュリティ機能は、AV2接続が消失したとき動作します。この場合において、テレビジョン受像機はPIN番号の入力なしでは動作しません。
このオプションを使用したいですか?
Yes
No
セキュリティ機能が始動されました!

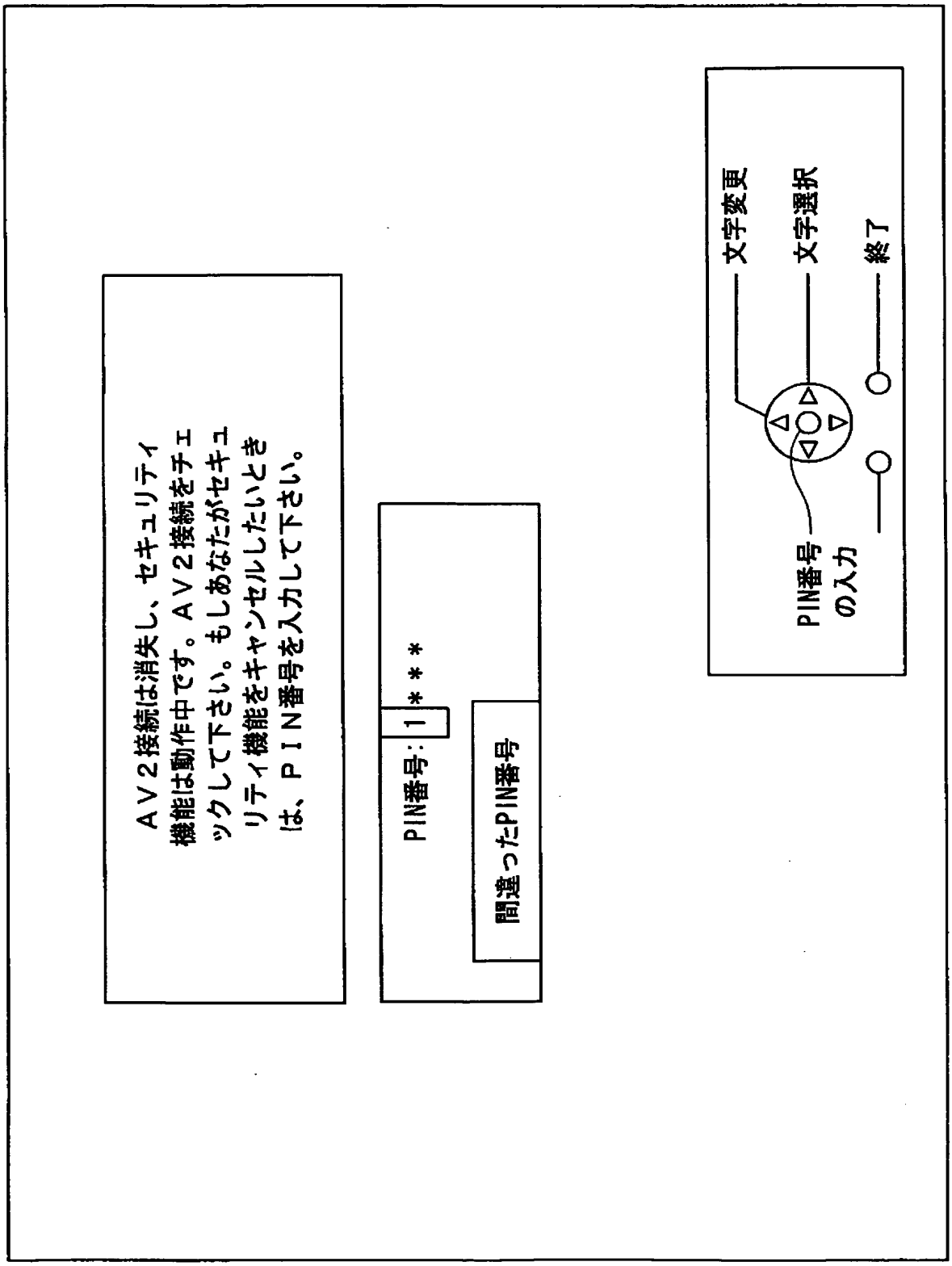
[図24]


画面D7：セキュリティオプションの使用の確認(5)
PIN番号"1234"で登録が完了しました。いま、同一のPIN番号でセキュリティ機能を起動させるためのオプションを得ました。セキュリティ機能は、AV2接続が消失したとき動作します。この場合において、テレビジョン受像機はPIN番号の入力なしでは動作しません。
このオプションを使用したいですか?
Yes
No
セキュリティ機能は、中止されました

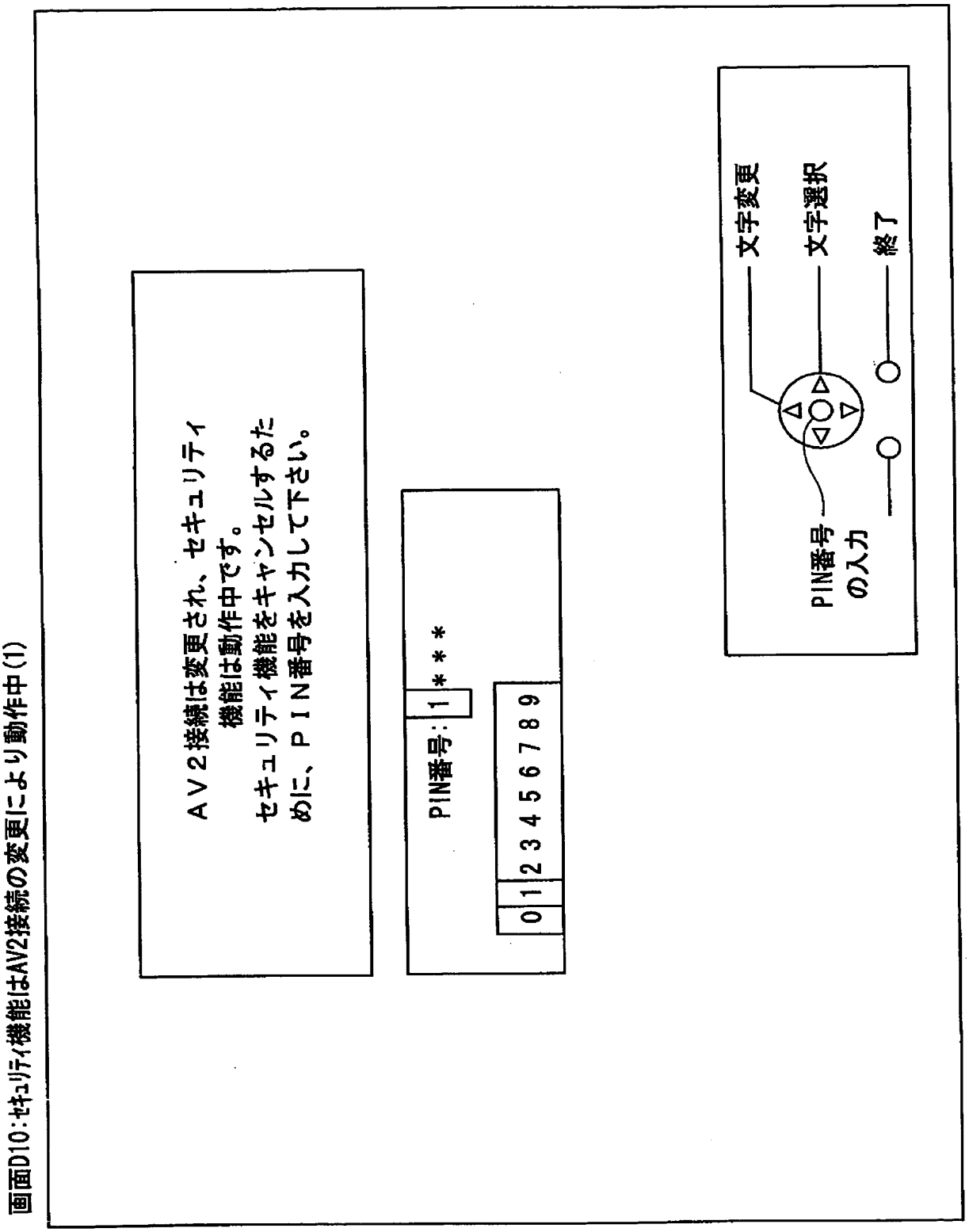
[図25]


画面D8：セキュリティ機能はAV2接続の消失により動作中(1)
AV2接続は消失し、セキュリティ機能は動作中です。AV2接続をチェックして下さい。もしあなたがセキュリティ機能をキャンセルしたいときは、PIN番号を入力して下さい。
PIN番号: 1***
0 1 2 3 4 5 6 7 8 9
文字変更
文字選択
終了
PIN番号の入力

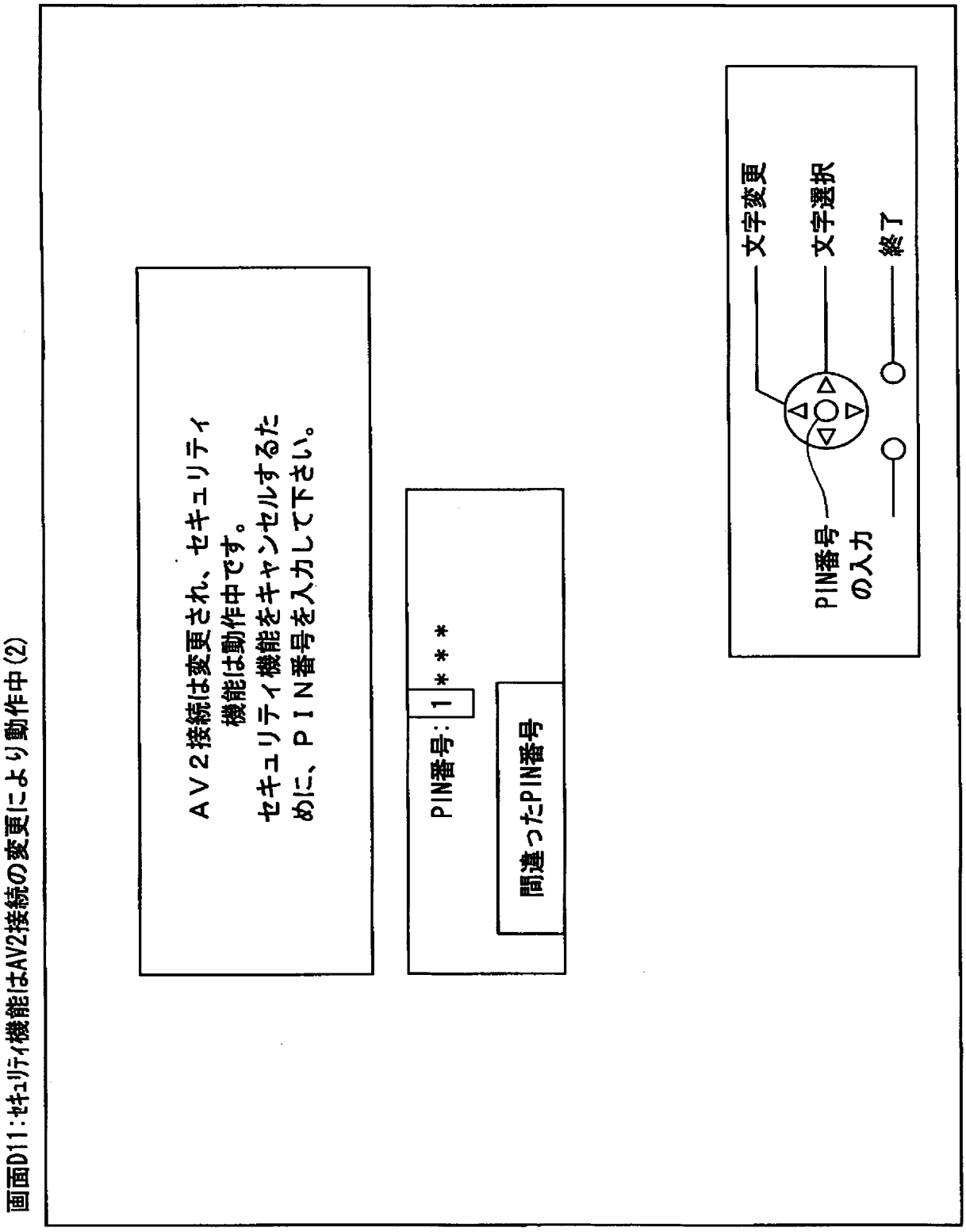
[図26]


画面D9：セキュリティ機能はAV2接続の消失により動作中(2)
AV2接続は消失し、セキュリティ機能は動作中です。AV2接続をチェックして下さい。もしあなたがセキュリティ機能をキャンセルしたいときは、PIN番号を入力して下さい。
PIN番号: 1 * * *
間違ったPIN番号
文字変更
文字選択
PIN番号の入力
終了

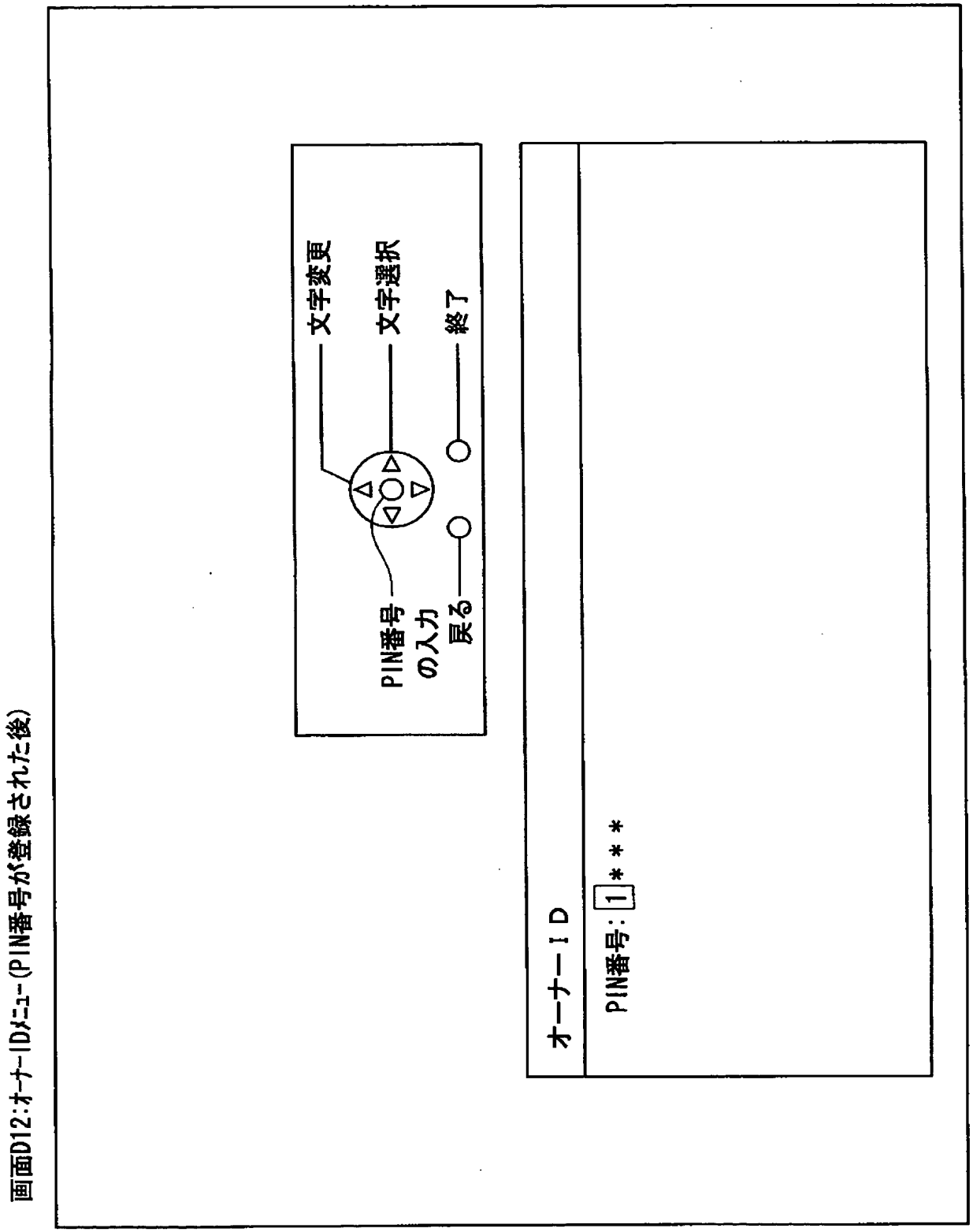
[図27]


画面D10:セキュリティ機能はAV2接続の変更により動作中(1)
AV2接続は変更され、セキュリティ
機能は動作中です。
セキュリティ機能をキャンセルするた
めに、PIN番号を入力して下さい。
PIN番号: 1 * * *
0 1 2 3 4 5 6 7 8 9
文字変更
文字選択
終了
PIN番号
の入力

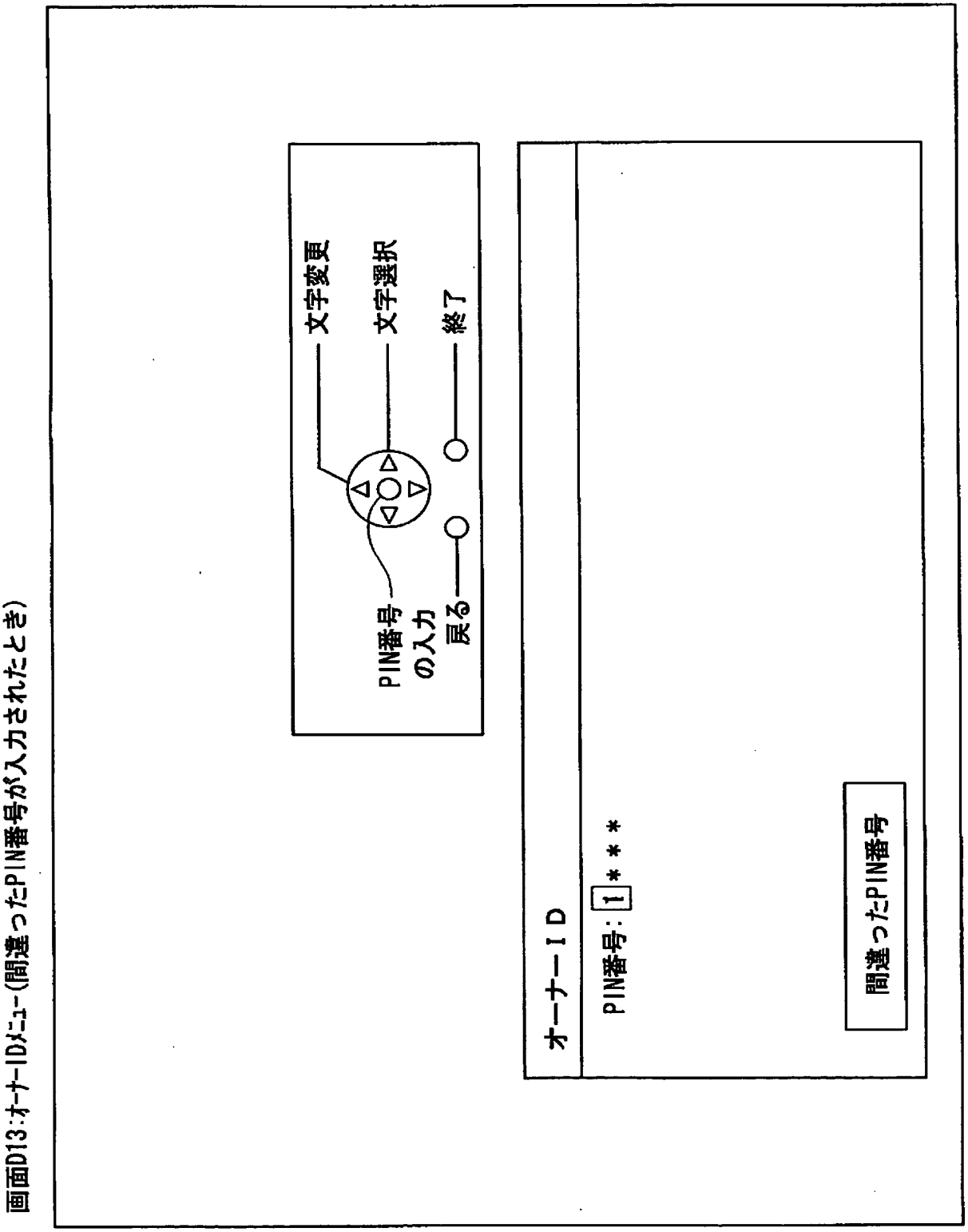
[図28]


画面D11：セキュリティ機能はAV2接続の変更により動作中(2)
AV2接続は変更され、セキュリティ
機能は動作中です。
セキュリティ機能をキャンセルするた
めに、ＰＩＮ番号を入力して下さい。
PIN番号: 1 * * *
間違ったPIN番号
文字変更
文字選択
終了
PIN番号
の入力

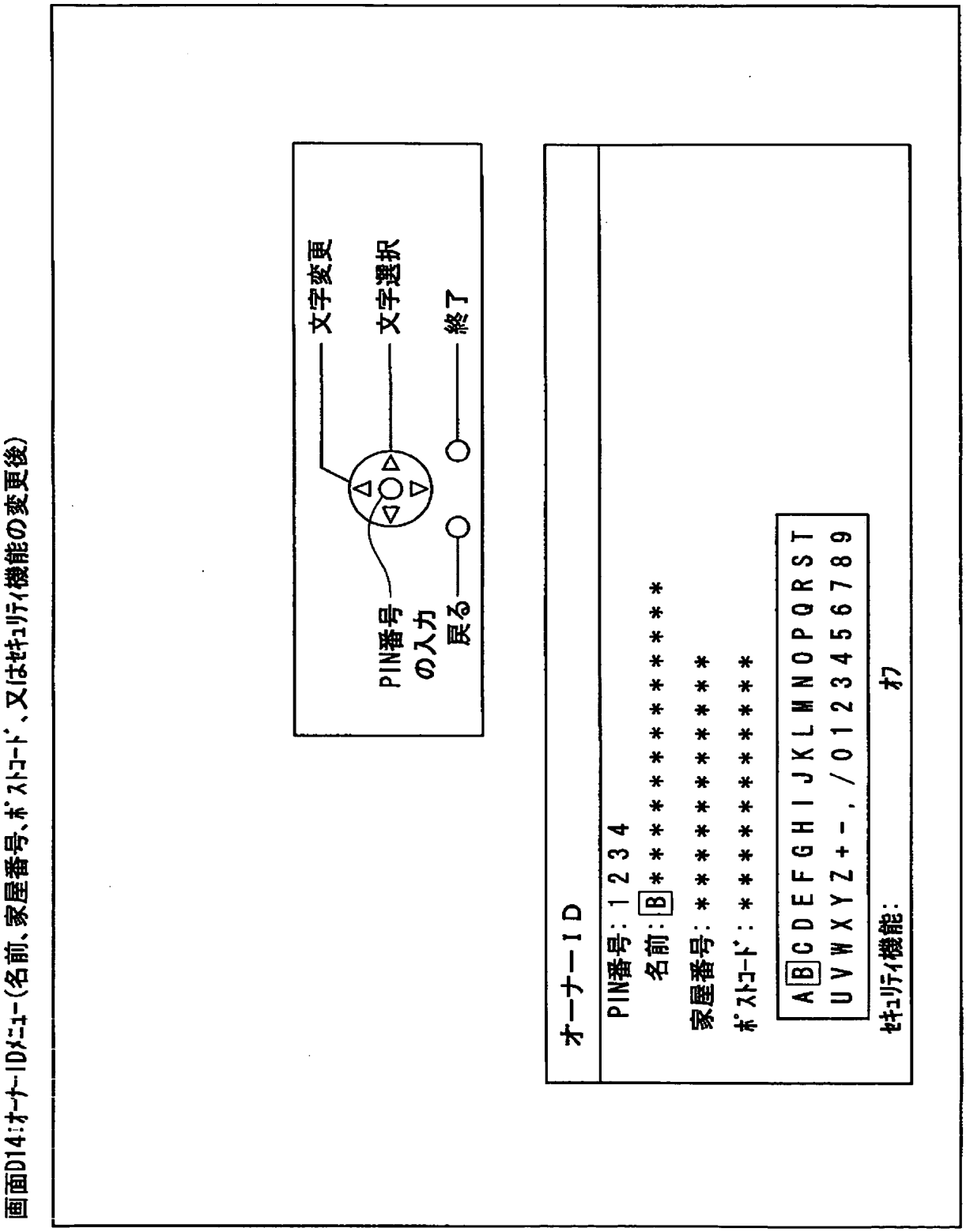
[図29]


画面D12:オーナーIDメニュー(PIN番号が登録された後)
オーナーＩＤ
PIN番号: 1 * * *
PIN番号の入力
戻る
文字選択
終了
文字変更

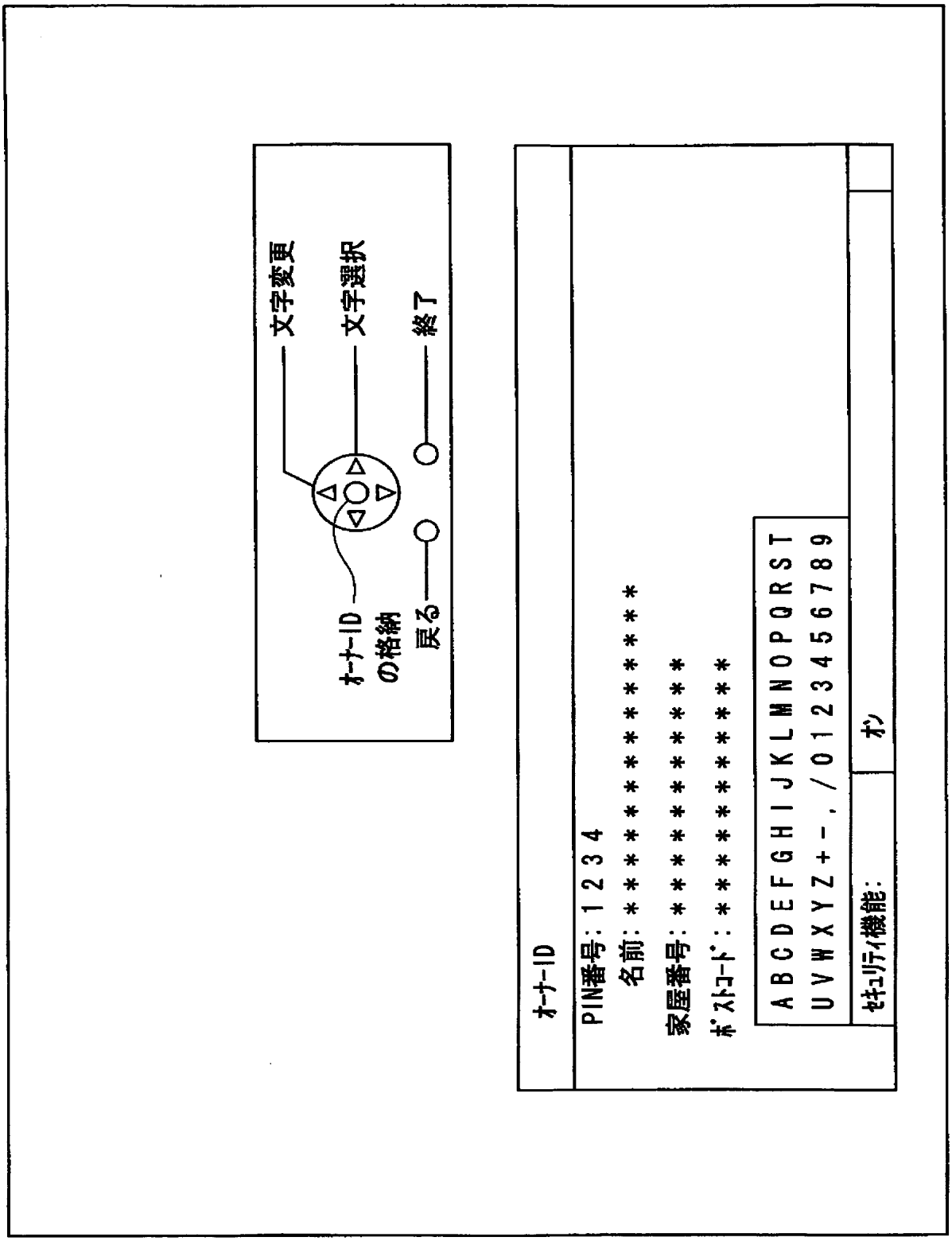
[図30]


画面D13:オーナーIDメニュー(間違ったPIN番号が入力されたとき)
オーナーID
PIN番号: 1 * * *
間違ったPIN番号
文字変更
文字選択
終了
PIN番号の入力
戻る

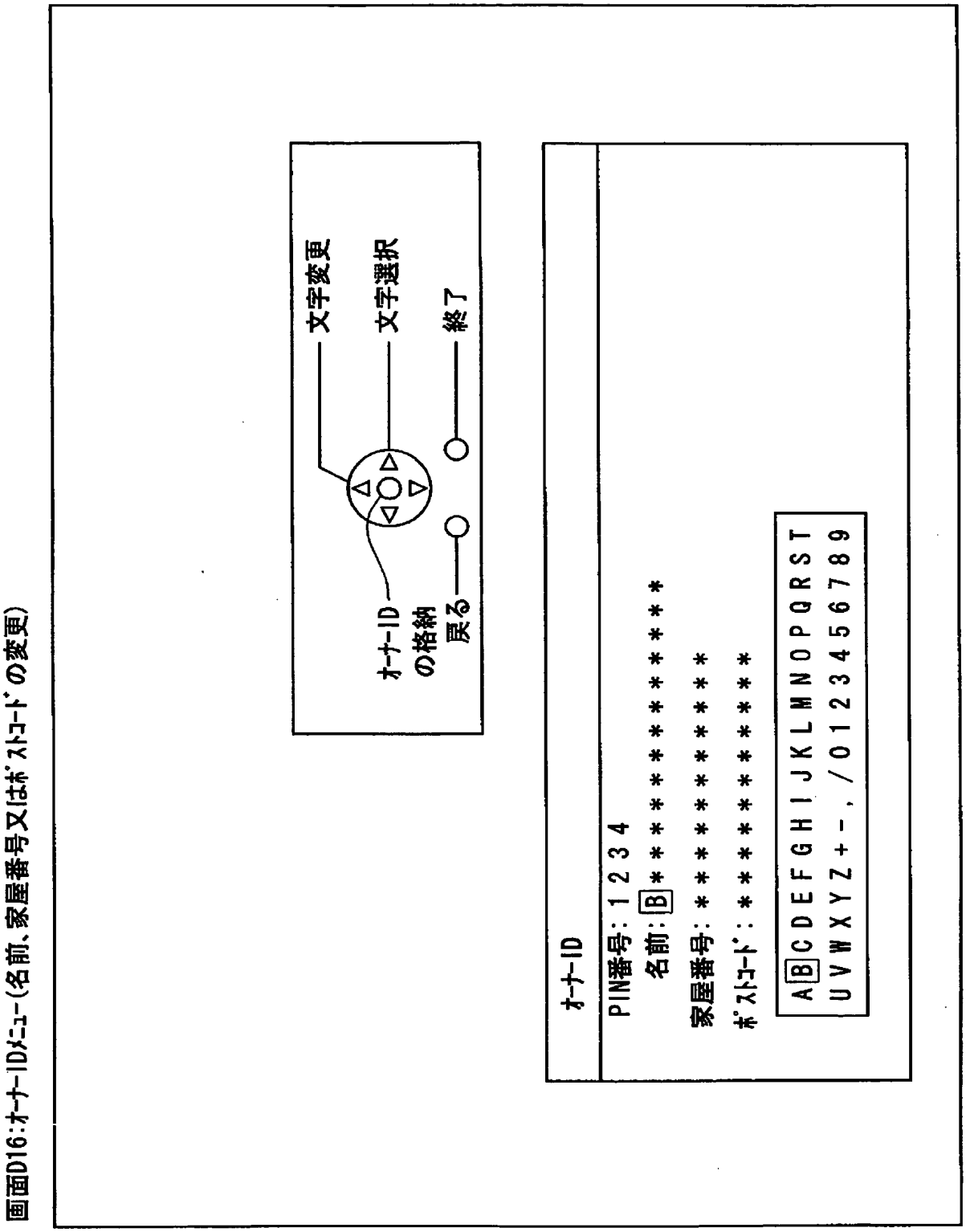
[図31]


画面D14:ｵｰﾅｰIDﾒﾆｭｰ(名前、家屋番号、ﾎﾟｽﾄｺｰﾄﾞ、又はｾｷｭﾘﾃｨ機能の変更後)
オーナーＩＤ
PIN番号: １２３４
名前: B＊＊＊＊＊＊＊＊＊＊
家屋番号: ＊＊＊＊＊＊＊＊＊＊
ﾎﾟｽﾄｺｰﾄﾞ: ＊＊＊＊＊＊＊＊＊＊
A B C D E F G H I J K L M N O P Q R S T
U V W X Y Z + － , / 0 1 2 3 4 5 6 7 8 9
ｾｷｭﾘﾃｨ機能: ｵﾌ
文字変更
文字選択
PIN番号
の入力
戻る
終了

[図32]


画面D15:オーナーIDメニュー(名前、家屋番号、ポストコード、又はセキュリティ機能の変更後)
オーナーID
PIN番号:1234
名前:**********
家屋番号:**********
ポストコード:**********
ABCDEFGHIJKLMNOPQRST
UVWXYZ+-.,/0123456789
セキュリティ機能:
オン
文字変更
文字選択
オーナーID
の格納
戻る
終了

[図33]


画面D16:オーナーIDメニュー(名前、家屋番号又はポストコードの変更)
オーナーID
PIN番号:1234
名前:B**********
家屋番号:**********
ポストコード:**********
ABCDEFGHIJKLMNOPQRST
UVWXYZ+-,/0123456789
文字変更
文字選択
オーナーID
の格納
戻る
終了

[図34]